

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
<small>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</small>					
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 24/May/2001		2. REPORT TYPE THESIS		3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE CONSTITUTIONAL CONFLICTS WITH ENCRYPTION REGULATION		5a. CONTRACT NUMBER			
		5b. GRANT NUMBER			
		5c. PROGRAM ELEMENT NUMBER			
		5d. PROJECT NUMBER			
6. AUTHOR(S) CAPT WINCHESTER REGINA S		5e. TASK NUMBER			
		5f. WORK UNIT NUMBER			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) UNIVERSITY OF COLORADO AT BOULDER			8. PERFORMING ORGANIZATION REPORT NUMBER CI01-90		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) THE DEPARTMENT OF THE AIR FORCE AFIT/CIA, BLDG 125 2950 P STREET WPAFB OH 45433			10. SPONSOR/MONITOR'S ACRONYM(S)		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION/AVAILABILITY STATEMENT Unlimited distribution In Accordance With AFI 35-205/AFIT Sup 1					
13. SUPPLEMENTARY NOTES					
20010720 015					
14. ABSTRACT					
15. SUBJECT TERMS					
6. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 126	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include area code)

CONSTITUTIONAL CONFLICTS WITH ENCRYPTION REGULATION

by

REGINA SENORA WINCHESTER

B.S., Purdue University, 1994

A thesis proposal submitted to the  
Faculty of the Graduate School of the  
University of Colorado in partial fulfillment  
Of the requirement for the degree of  
Masters of Arts  
School of Journalism and Mass Communication

2001

## DEDICATION

This thesis is dedicated to my parents, Robert and Judy Winchester. Without their help, support, and love, I would not be where I am today. Thank you for making me look it up, do it myself, and, ever against my will, build my own character.

Winchester, Regina S. (M.A., School of Journalism and Mass Communication)

## Constitutional Conflicts With Encryption Regulation

Thesis directed by Prof. Robert Trager

The government's need to control and have access to information has resulted in attempts to regulate the use of strong encryption over the Internet. The government argues that national security requires this control to stop terrorists, child pornographers, and drug traffickers from preventing government access to online communications. These regulations fail to take into account the history of encryption as a military and National Security Agency tool, and encryption's subsequent entrance into the public and private sphere. Regulation and control isolate the Internet as a form of communication and target it in ways that would not be allowed in other media. The controls in place and suggested are overly intrusive without showing adequate justification for being so, and affront current notions of First Amendment and privacy rights. The focus of this thesis is to describe the evolution of encryption from military to private use, and the failure of government regulations to recognize and adapt to that change. The thesis argues that government refusal to allow strong encryption for non-military Internet communication cannot be justified.

## CONTENTS

### CHAPTER

1.	INTRODUCTION .....	1
2.	COURT DECISIONS AND ENCRYPTION LEGISLATION .....	5
	Court Decisions .....	6
	Clinton Administration Legislation .....	10
	Other Government Monitoring Systems .....	15
	Law Enforcement Issues .....	17
	Encryption as a Munition .....	19
	Military Uses of Encryption .....	21
	Privacy Issues .....	22
	Historical Perspectives .....	24
	Research Questions .....	26
	Methodology .....	27
3.	HISTORY OF THE MILITARY, NSA, AND THE INTERNET ....	29
	History in Wartime .....	29
	NSA Uses of Cryptography .....	31
	NSA, DoD Regulations .....	34
	The ARPANET .....	35
	How Encryption Works .....	36
	A Flourishing Internet .....	37
	Foundation of Encryption Regulations .....	39

4.	FEDERAL AND MILITARY ENCRYPTION REGULATION .....	42
	DoD and Military Regulations .....	43
	Encryption as a Munition, and International Agreements About Export of Such Technologies .....	46
5.	CHANGES IN ENVIRONMENT AND ENCRYPTION REGULATION .....	51
	Legislation Timeline .....	52
	Change in Classification .....	55
	CESA Of 1999 and Export Regulation Changes .....	59
	Encryption Litigation .....	61
	Concerns About CESA and 2000 Regulations .....	67
	Previous Relevant Cases .....	68
6.	THE GOVERNMENT'S UNCOMPROMISING ENCRYPTION REGULATIONS .....	71
	Fear of Criminal Use of Encryption .....	71
	Attempts to Limit Development, Exportation, and Domestic Use of Encryption .....	74
7.	SOCIAL AND POLITICAL PROBLEMS WITH REGULATION .....	77
	Moving Beyond Old Customs .....	77
	Need for Privacy and Security for Information Transfer .....	78
	National Security as Priority, But Not at Expense of Free Speech, Privacy .....	81
	Reasonable Expectation of Privacy Over the Internet? .....	83
	Market Dominance in Product Development .....	86
	Outside Availability of Encryption Products .....	88

	Federal Uses and the Law of Unintended Consequences ....	91
8.	PROBLEMS WITH USING EXISTING MONITORING METHODS AS PRECEDENTS FOR INTERNET SURVEILLANCE .....	94
	Courts and the Rapidly Changing Technology .....	94
	The Electronic Communications Privacy Act of 1986 .....	97
	CALEA as Precedent for Internet Monitoring .....	98
	Attempts to Transfer Pen Register, Wiretapping to Internet	100
	Fourth Amendment Conflicts With Electronic Surveillance, and Encryption Limitations .....	104
9.	CONCLUSIONS AND RECOMMENDATIONS .....	108
	Conclusions .....	108
	Bottom Line .....	114
	Limitations of This Study.....	116
	Suggestions for Further Research .....	118
	BIBLIOGRAPHY .....	120
	APPENDIX: LIST OF ACRONYMS USED .....	126

## CHAPTER 1

### INTRODUCTION

Today there are many contentious issues at stake in the regulation of communication encoding – as seen in military versus private and business uses, and the fight over whether the ultimate need to secure privacy for citizens’ and business uses can override government desire to enhance public safety and national security. Encryption<sup>1</sup> has traditionally had specific rules for wartime and military uses that did not apply to private citizen or corporate uses – the question arises as to why the rules for military use should be applied outside the military complex.

This thesis will not argue for a system in which encryption use over the Internet is not regulated at all. Rather, it will agree with John. L. Huffman et al. in the article “Encryption and the First Amendment” (discussed in greater detail in further chapters). The authors point out the many faults with the Clinton administration regulations, the lack of justification for such strict restrictions, and the need for recognition of Constitutional rights to be reflected in such regulations.

Historically, though small-scale (compared to Internet use), businesses and private citizens have used means of encryption to send coded messages and ensure their privacy – over the telegraph, in writing (in newspapers and letters), and through other media – all apparently without any notable regulation by the government. Some might argue that this was because private methods would not have withstood a

serious attempt to decrypt them, and now that the Internet offers more privacy, ironically the government sees *more* justification for limiting that privacy. National Security Agency (NSA) and military schemes for control over information are very rigorous. Members of these organizations are subject to strict control and monitoring, and follow specific protocols for the transfer and handling of information. These security measures have to do with the importance of maintaining control over information, especially federally classified information, in the interests of national security. While security is also important in the public sector, members of the public have not been subject to such limitations – as often they would drastically conflict with First Amendment rights.

The government clearly has an interest in maintaining secure but government-decipherable encryption schemes in its ongoing use in military, NSA, and other intelligence applications. This has been the standard for encryption use in the past, and should remain in place for such uses. There is an entire array of regulations, manuals, laws, and customs in place to secure information and the transfer of information, on the handling of sensitive information, on the unauthorized release of classified information, on the transmission and reception of such information, and on attempts to intercept and decrypt foreign intelligence information. However, this thesis argues these laws and regulations should remain firmly fixed in the realm in which they were developed, and not imposed on private and commercial use.

---

<sup>1</sup> Encryption is the use of a secret code for the translation of data into ciphertext, which is unreadable by anyone who does not know the key to unencrypt the data. See Chapter 3 for more information.

Today, the government needs a warrant or a court-order in order to wiretap a telephone line and to intercept a phone conversation.<sup>2</sup> To intercept written communication is a federal offense, and there exists no substantial precedent for prohibiting the use of scrambled local signals, as in using amateur radio signals. Privacy law protects people, not places<sup>3</sup> – so people and their communications in cyberspace ought to be offered the same protections against intrusion. This is true now more than ever, since it has been established in recent court cases that speech over the Internet earns the highest degree of First Amendment protection available,<sup>4</sup> and that even computer code and encryption codes are a form of speech (and entitled to First Amendment protections).<sup>5</sup> The courts have established a right to speak freely over the Internet – the issue this brings up is whether there is a reasonable expectation of privacy on the net, and how encryption legislation conflicts with that privacy.

It is true that there are different regulations for different media, from newspapers to broadcast to motion pictures, but the Internet has been determined to

---

<sup>2</sup> 29 *Electronic Surveillance -- Title III Affidavits* (visited Nov. 7, 2000) <[http://www.usdoj.gov/usao/eousa/foia\\_reading\\_room/usam/title9/crm00029.htm](http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00029.htm)>, which outlines requirements for such surveillance.

<sup>3</sup> *Katz v. United States*, 389 U.S. 347, at 353.

<sup>4</sup> *Reno v. ACLU* 521 U.S. 844 (1997).

<sup>5</sup> Bernstein filed suit challenging the constitutionality of the ITAR regulations, resulting in the first decision, *Bernstein v. Department of State*, 922 F. Supp. 1426 (N.D. Cal. 1996) (*Bernstein I*). The district court found that the source code was speech protected by the First Amendment, and granted summary judgment to Bernstein on his First Amendment claims, holding the challenged ITAR regulations facially invalid as a prior restraint on speech, see *Bernstein v. Department of State*, 945 F. Supp. 1279 (N.D. Cal. 1996) (*Bernstein II*). In December 1996, President Clinton shifted licensing authority for nonmilitary encryption commodities and technologies from the State Department to the Department of Commerce. The Department of Commerce then promulgated regulations under the EAR to govern the export of encryption technology, regulations administered by the Bureau of Export Administration. Bernstein subsequently amended his complaint to add the Department of Commerce as a defendant, advancing the same constitutional objections as he had against the State Department. The district court once again granted summary judgment in favor of Bernstein, finding the new EAR regulations facially invalid as a prior restraint on speech. See *Bernstein v. Department of State*, 974 F. Supp. 1288 (N.D. Cal. 1997) (*Bernstein III*). The Ninth Circuit published another decision in favor of Bernstein, see 176 F.3d. 1132 (9th Cir. 1999), but this was later withdrawn for en-banc review. See 192 F.3d. 1308 (9th Cir. 1999). The case remains pending.

receive much more First Amendment freedom than, for example, the more regulated broadcast media. These broadcast restrictions could not apply to the Internet since it is not a scarce resource, and any attempt to regulate the content over the Internet conflicts with First Amendment protections. Another important issue is the alleged difference between the Internet and other media. The main distinctions seem to revolve around the Internet's speed and reach. However, that the Internet may result in a more efficient criminal is not enough justification for regulating everyone's communication. People will still be able to use the "one-off" codes, or codes with a non-digital encryption and decryption means, to communicate information – which does not fit into any of the legislation regarding use of digital encryption.

## CHAPTER 2

### COURT DECISIONS AND ENCRYPTION LEGISLATION

Much of the existing literature relating to encryption regulation in the United States focuses on the constant changes during the Clinton administration, and the continuing objections by business, privacy rights organizations, and private citizens. There are significant studies of the three ongoing court cases protecting computer source code as speech and other First and Fourth Amendment implications of encryption regulation. Finally, much existing work is focused on the issues of privacy confronted by the concept of mandatory back doors (where encryption software is written in such a way that there is another “back door” way to go in and decrypt the information without the proper key) and key escrow schemes (in which a copy of a person’s or businesses’ private key is held by a third party), and the attempts at limiting domestic use of strong encryption.

There has never been a precedent establishing that for all communication the government has a complete and unabridged right to know what the content of that communication is, even if the communication is in the furtherance of a crime. The use of encryption in various forms can be traced back to earliest civilizations. While each new communication technology has brought with it new paranoias, rules and regulations, no medium has been so straightforwardly subject to the kind of government involvement illustrated by the regulations affecting encryption use on the Internet. Also, there are few precedents for attempting to impose military controls

over information onto the general public. Few studies focus on the basic imposition of Department of Defense regulation onto the public. Commentators instead are focusing on what the extent of the regulations should be, which is important - but there are other, more basic questions to be addressed first – such as why such strict regulations are in place over private and public communication; why the Internet has been targeted for this kind of regulation; and what the evolution of the Internet has done to changing ideas of appropriate legislation concerning encryption use.

### **Court Decisions**

The three cases relating to encryption as speech and as protected despite current government regulations are the cases of *Bernstein v. United States Department of Justice*,<sup>6</sup> and *Karn v. U.S. Department of State*,<sup>7</sup> and *Junger v. Daley*.<sup>8</sup> Below is a sketch of each of the cases, which will be more fully explained in Chapter 5. The *Bernstein* case was the most famous, and resulted in a finding of source code as protected speech, although the case remains under appeal by the government. The code was for an encryption method that Daniel Bernstein, a professor in the Department of Mathematics, Statistics, and Computer Science at the University of Illinois at Chicago, developed and posted on the Internet. A second district court decided the code was speech, and as such received First Amendment protection, and that the restrictions found under the International Traffic in Arms Regulations

---

<sup>6</sup> *Bernstein v. Department of State*, 922 F. Supp. 1426 (N.D. Cal. 1996) (*Bernstein I*).

<sup>7</sup> *Karn v. U.S. Department of State*, 925 F.Supp. 1 (D.D.C. 1996). *Remanded*, No. 96-5121, 1997 U.S. App. LEXIS 2123, at \*1 (D.C. Cir. Jan 1997) (for consideration of transfer of regulatory authority to U.S. Department of Commerce).

<sup>8</sup> *Junger v. Daley*, 8 F. Supp. 2d 708 (N.D. Ohio 1998).

(ITAR)<sup>9</sup> – which said that Bernstein would need a license to export the paper, source code, or instructions – were equivalent to a prior restraint.<sup>10</sup>

It has been pointed out that Bernstein fared a bit better in his challenge of the constitutionality of the same regulations at issue, preventing American researchers and companies from exporting cryptographic software and hardware. He wrote an academic paper discussing his algorithm and source code<sup>11</sup> implementing the algorithm, and wanted to present talks about it at conferences and on the Internet. The Office of Defense Trade Controls declared that his system was considered a defense article, and subject to a licensing requirement before it can be exported. Not knowing which elements this decision referred to, Bernstein requested a separate determination as to five distinct elements – the paper, the two software components, and two texts on implementation and use of the algorithm. The response to his request was that all of the elements constitute defense articles. This determination resulted in *Bernstein v. United States Department of State*. After the suit was filed, the Office of Defense Trade Controls wrote to Bernstein to “clarify” that its determination applied only to the software elements, and not to the texts. Later trials were to consistently favor Bernstein’s rights, but the case remains under appeal.

Peter Junger, plaintiff in another case, is a law professor teaching a computer course at Case Western Reserve University Law School. Junger maintained a website to which he posted class information and other items of interest to him, and he wanted to post to his website encryption source code that he had developed. He requested

---

<sup>9</sup> 22 C.F.R. pts. 120-130 (1995).

<sup>10</sup> *Bernstein v. Department of State*, 974 F. Supp. 1288 (N.D. Cal. 1997) (*Bernstein III*), 974 F. Supp. at 1310.

that the Commerce Department determine whether or not such a posting would require a license under ITAR. Because under ITAR almost any posting of software on the Internet is an export, the Commerce Department determined on July 4, 1997, that Junger would need a license. Junger brought an action claiming the licensing scheme was an invalid prior restraint on his right to speak freely.

The court rejected Junger's arguments and granted the government's summary judgment motion.<sup>12</sup> In reaching this result, the Junger court set up a standard that differentiated between expressive and functional activity. In other words, activity with communicative purposes and characteristics should be protected as speech, but activity intended to perform some nonexpressive function should not be protected. The most important issue, as the court saw it, was "whether the export of encryption software source code is sufficiently expressive to merit First Amendment protection."<sup>13</sup> The court did not provide a clear definition of what activity qualified as "sufficiently expressive." However, it did determine that "inherently expressive.... software contains an "exposition of ideas,"" which would presumably qualify as sufficiently expressive for free speech protection. At the same time, the court indicated that inherently functional software would not meet the sufficiently expressive standard. The court held that encryption source code was "inherently functional" and its exportation was not protected by the First Amendment.<sup>14</sup> It was

---

<sup>11</sup> Source code refers to the text of a computer program written in a "high-level" programming language, such as Pascal or C. Source code is meant to be read by humans, where a computer can make no direct use of source code until it has been compiled into a "machine" language (object code).

<sup>12</sup> Junger v. Daley, 8 F. Supp. 2d 708 (N.D. Ohio 1998).

<sup>13</sup> *Id.*, at 715.

<sup>14</sup> *Id.*

not until April 2000 that this decision was reversed and remanded back to the district court.<sup>15</sup>

In *Karn*, like *Bernstein*, a federal district court was presented with the issue of whether the Department of State can constitutionally restrict certain forms of encryption or whether the materials at issue constituted speech and would be entitled to protection under the First Amendment. Philip Karn's case concerned whether a computer disk containing encryption code is a defense article under the Arms Export Control Act<sup>16</sup> (AECA) and ITAR, and is thus subject to a licensing requirement in order to export the disk.<sup>17</sup> Karn filed a request to export the book "Applied Cryptography" by Bruce Schneier. The book explains different aspects of cryptography – history, politics, different encryption algorithms, and techniques to implement cryptographic algorithms. One part of the book contains computer source code for a number of cryptographic algorithms. Stuck in the back of the book was also a computer disk containing the same source code found printed in the book. The Department of State's Office of Defense Trade Controls declared that it did not have jurisdiction under the ITAR as to the book, but did *not* extend this determination to the disks. Karn's challenge to the regulations claimed they violated his free speech rights, but the court decided the regulations were content-neutral and his claim was rejected.<sup>18</sup>

The Electronic Frontier Foundation is a non-profit organization working in the public interest to protect fundamental civil liberties, including privacy and freedom of

---

<sup>15</sup> *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000).

<sup>16</sup> Arms Export Control Act, 22 U.S.C. §§ 2751-2799aa-2.

<sup>17</sup> *Karn v. U.S. Department of State*, 925 F.Supp. 1 (D.D.C. 1996), at 3-4.

<sup>18</sup> *Id.* at 12.

expression in the arena of computers and the Internet.<sup>19</sup> EFF holds the *Bernstein* judgements as a victory for First Amendment rights.<sup>20</sup> Judge Marilyn Hall Patel's decision struck down Cold War export restrictions on the privacy technology of cryptography, and knocked out a major part of the Clinton administration's effort to force companies to build "wiretap-ready" computers, set-top boxes, telephones, and consumer electronics. The regulations in question also defined "export" to include simple publication in the U.S., as well as discussions with foreigners inside the U.S.; and define "software" to include printed English-language descriptions and diagrams, as well as the traditional machine-readable object code and human-readable source code. According to EFF, the decision went toward a victory for free speech, academic freedom, and the prevention of crime – because American scientists and engineers would be more free to collaborate with their peers in the United States and in other countries, enabling them to build a new generation of tools for protecting the privacy and security of communications.

### **Clinton Administration Legislation**

Civil libertarians and organizations like the EFF argue that encryption should be widely deployed on the Internet and throughout society to protect privacy, prove the authenticity of transactions, and improve computer security. Industry has argued that the restrictions hobble them in building secure products, both for U.S. and worldwide use, risking America's current dominant position in computer technology.

---

<sup>19</sup> *General Information About the Electronic Frontier Foundation* (visited Feb. 20, 2000) <<http://www.eff.org/abouteff.html>>.

<sup>20</sup> *Court Declares Crypto Restrictions Unconstitutional: Free Speech Trumps Clinton Wiretap Plan*, (last modified Dec. 19, 1996) <[www.eff.org](http://www.eff.org)>.

However, even these organizations acknowledge one of the government justifications for encryption regulations – that these technologies provide privacy to criminals as well as ordinary citizens.

The Clinton administration has been criticized for attempts to use the export restrictions to force companies into building wiretap-ready key recovery technology, in particular with a November 1996 executive order, which offered limited administrative exemptions from these restrictions to companies which agree to undermine the privacy of their customers. NSA laws, regulations, and standards were said to have been used to force, persuade, or confuse individuals, companies, and government departments into making it easy for NSA to wiretap and decode all kinds of communications. However, in recent years these rules appear to have declined in the face of increasing visibility, vocal public disagreement with the agency's goals, commercial and political pressure, and judicial scrutiny.

A 1997 article discusses the background and timeline of Clinton administration attempts to regulate the Internet.<sup>21</sup> It begins by describing cryptography as once being an area of interest largely for government agencies, which has now entered the mainstream world of the Internet. This presented an intense effort on the part of governmental agencies to control the means of communication. Against a backdrop of increasing instances of domestic terrorism, pressure from law enforcement agencies, and a software industry and Congress hostile to administration efforts to restrict the export of encryption technology, the Clinton administration made numerous attempts to establish standards for the encryption of voice and data communication over the rapidly growing Internet.

The article describes how in 1997 the Clinton administration reached a critical juncture in its efforts to balance free speech and privacy with the needs of law enforcement and national security. It argues that administration efforts to create and impose an encryption standard through the Clipper regime were flawed and unconstitutional. Combined with external and internal pressures, the administration was trapped in the position of trying to impose an encryption standard on something as vast and as difficult to regulate as the Internet.

However, other studies detail how several senators, supported by Federal Bureau of Investigation (FBI) Chief Louis Freeh, favored imposing domestic limits on computer encoding technology.<sup>22</sup> From the senators' point of view, encryption programs have become an increasingly important means of securing electronic commerce and communications – but they bring up the recurring idea that scrambling capability could also be used by criminals to hide their dealings from law enforcement agencies. Sen. Dianne Feinstein (D-Calif.) said she would favor requiring manufacturers of encryption products to include features allowing the government to decode any message by recovering the software keys, saying, “Nothing other than some kind of mandatory key recovery really does the job.”<sup>23</sup> Freeh told the subcommittee he would also favor mandatory key recovery, but added that such a policy was probably unattainable given the strong opposition from other lawmakers and interest groups.<sup>24</sup>

---

<sup>21</sup> John L. Huffman et al., *Encryption and the First Amendment*, 2 COMM. L. AND POLICY (1997).

<sup>22</sup> See, e.g., Aaron Pressman, *Senators Call For Mandatory US Encryption Controls*, Sep. 4, 1997.

<sup>23</sup> *Id.*

<sup>24</sup> *Id.*

There were attempts at compromise over net regulation.<sup>25</sup> The E-PRIVACY Act was one such attempt, introduced on May 12, 1998, by Senators Patrick Leahy and John Ashcroft.<sup>26</sup> This act would have allowed companies to export advanced encryption products, and would have barred domestic controls, while also attempting to address concerns voiced by law enforcement. This bill and others tried to reconcile differing points of view: computer users and privacy advocates arguing that the technology is necessary to secure electronic communications and data, keeping information safe from prying eyes, while government agencies counter that encryption allows criminals to communicate with impunity. The point of view of software developers was also considered, complaining that government restrictions barring the export of advanced encryption products had hindered their ability to compete in a world market where the technology is readily available from foreign vendors.

The bill proposed allowing for the export, after a one-time review, of mass-market encryption products. Custom technology could be exported provided that comparable foreign-made products are already available. Exports for military uses and to embargoed countries such as Cuba and North Korea would have been restricted. Domestic users would be free to use any encryption product, and government-mandated key recovery systems would have been barred, unlike previous proposals – and in marked difference to such arguments that recovery systems, where a third party would hold the key to an encryption product and be forced to turn it over under certain conditions, are vital to national defense. Yet other provisions of the E-

---

<sup>25</sup> *Monday E-Privacy Act Attempts Encryption Compromise*, N.Y. L.J., May 18, 1998, at S11.

PRIVACY Act were designed to assist law enforcement efforts, by making it a criminal offense to use encryption to hide incriminating evidence.

A United States Department of Commerce press release in January 2000 provided an explanation of the newer Clinton initiatives.<sup>27</sup> The Department of Commerce Bureau of Export Administration (BXA) issued new encryption export regulations which implement the new approach initially announced by the Clinton Administration in September 1999. The changes permit U.S. companies to export any encryption product around the world to commercial firms, individuals and other non-government end-users under a license exception (i.e., without a license). In addition, retail encryption products which are widely available in the market can be exported to any end-user including foreign governments, although a one-time product review by BXA continues to be required. “We’ve also worked very hard to address privacy concerns and to ensure that our law enforcement and national security concerns are met,” said Commerce Secretary William M. Daley.<sup>28</sup> The release also seemed to take into account the 1999 Bernstein<sup>29</sup> decision, saying that for source code, the regulation reduced control even further than announced in September. Commercial encryption source code, encryption toolkits, and components can be exported under license exception to businesses and non-government end-users for internal use and customization and for the development of new products. In addition,

---

<sup>26</sup> Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E-PRIVACY) Act, S.2067, 105th Cong. (1998).

<sup>27</sup> *Commerce Announces Streamlined Encryption Export Regulations*, United States Department of Commerce press release (last updated Jan. 12, 2000) <<http://204.193.246.62/public.nsf/docs/60D6B47456BB389F852568640078B6C0>>.

<sup>28</sup> *Id.*

<sup>29</sup> Bernstein, 176 F.3d. 1132 (9th Cir. 1999).

the regulations relax restrictions on publicly available encryption source code, including by posting on the Internet.

The new regulation permits exports of any encryption item to their foreign subsidiaries without a prior review. Foreign employees of U.S. companies working in the United States no longer need an export license to work on encryption. The new changes did not affect restrictions on terrorist supporting states (Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria), their nationals, and other sanctioned entities. In addition, the guidelines also implement agreements reached by the Wassenaar Arrangement<sup>30</sup> in December 1998 by decontrolling 64-bit mass market products and 56-bit encryption items.<sup>31</sup>

### **Other Government Monitoring Systems**

A 1996 CATO Institute paper talks about the 1994 Communications Assistance in Law Enforcement Act (CALEA)<sup>32</sup> and the reality of federal wiretapping provisions that Congress had voted *against* earlier (in 1991) being tacked onto an omnibus appropriations bill.<sup>33</sup> CALEA gave the FBI power to demand that telephone companies rebuild their networks to make wiretapping easier. Other measures proposed for passage in the omnibus bill included a provision allowing law

---

<sup>30</sup> The Wassenaar Arrangement is the first global multilateral arrangement covering both conventional weapons and sensitive dual-use goods and technologies. Named after a suburb of The Hague, Netherlands, where agreement was reached to establish the international arrangement on export controls, the Arrangement received final approval by 33 co-founding countries in July 1996 and began operations in September 1996. It is headquartered in Vienna, Austria.

<sup>31</sup> 56-bit and 64-bit refer to the relative lengths of the key required to decrypt the encoded data. The longer the key, the more secure the encryption.

<sup>32</sup> Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in sections 18 U.S.C. and 47 U.S.C.).

<sup>33</sup> Solveig Bernstein, *Democracy Betrayed Means New Wiretapping Powers* (visited Apr. 20, 2000) <[www.cato.org/dailys](http://www.cato.org/dailys)>.

enforcement officers to use roving wiretaps without getting permission from a court to do so. This means that the police could tap a telephone without a warrant if they saw someone they thought might be a criminal enter a house or place of business. Another proposed rule would allow investigators to use emergency wiretaps, which could be used for 48 hours without a warrant, even when there is no emergency. The paper argues that the suggested changes to the emergency rule would vastly expand the types of cases in which police could wiretap without a warrant. Currently, the police can use emergency wiretaps in cases involving organized crime, national security, or to prevent immediate risk of injury. The new rule would allow emergency wiretaps to combat anything the government might call terrorism, even when there is no immediate risk of injury or a threat to national security. With judges available to authorize wiretaps 24 hours a day, in fact there is no reason for police to wiretap without a warrant for two entire days, when there is no immediate risk of injury.

Another monitoring system which has caused much concern is the FBI's Carnivore. Carnivore is a filtering tool which the FBI has developed to conduct electronic surveillance of electronic communications occurring over computer networks. In particular, it enables the FBI to conduct both full communications' content interceptions and pen register and trap and trace investigations to acquire addressing information.<sup>34</sup> According to the FBI, Carnivore is a system to help combat acts of terrorism, espionage, information warfare, hacking, and other serious

---

<sup>34</sup> *Carnivore Diagnostic Tool, Statement for the Record Before the United States Senate The Committee on the Judiciary*, 106th Cong. (2000) (statement of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation).

and violent crimes occurring over the Internet, acts which threaten the security of the nation.<sup>35</sup>

There has been much concern about the use of this system, primarily focusing on the ideas that (1) through its use of Carnivore, the FBI is collecting more information than a given (low standard) pen register<sup>36</sup> or trap and trace court order permits, or (2) while using Carnivore, the FBI is acquiring more information under such order than that order *should* lawfully permit.<sup>37</sup>

### **Law Enforcement Issues**

The Pacific Research Institute for Public Policy,<sup>38</sup> an institute which focuses on public policy issues such as education, the environment, law, economics, and social welfare, produced an excellent summary of encryption policy in the United States (as of May 1998).<sup>39</sup> The report says businesses and individuals need to be confident that their data and communications are secure if the information age is to reach its potential, and that encryption programs are the key to this security. The conflict between the use and abuse of the security is acknowledged. While encryption protects information from criminals, it also protects criminals from the police. Just as legitimate transactions can be encrypted, so can communications between spies, drug traffickers, and terrorists. The report points out that U.S. law enforcers fear that, by protecting criminal communications, strong encryption

---

<sup>35</sup> *Id.*

<sup>36</sup> 29 *Electronic Surveillance -- Title III Affidavits*, *supra* note 2, which illustrates that historical information combined with pen register information is still generally insufficient to establish probable cause under existing Department of Justice policy.

<sup>37</sup> *See id.*

<sup>38</sup> *Mission Statement* (visited Feb. 20, 2000) < <http://www.pacificresearch.org/>>.

jeopardizes national security. It is in response to this fear that the government has implemented policies that restrict the manufacture, distribution, and use of strong encryption. The report brings up the policy of eliminating all regulations on encryption. This would not only assure the security of legitimate transactions, it also would empower law enforcers to respond to computer crimes with market-driven innovations instead of government-imposed regulations.

The report concludes that encryption programs are the key to the security of the information age, and that the market for encryption is large and growing. It also argues that the restrictive policies will not accomplish the goal of preventing the proliferation of encryption by criminals. Even if strong encryption were banned, criminals could still use several means to acquire it: they could use it from sources abroad, acquire it from Internet-based, hidden sources, contract programmers to develop encryption for them, or create the programs themselves.

A CNET news article posted in August 1998 explains the national security concern, focusing on the impact terrorism has on government drive to regulate Internet communications.<sup>40</sup> It discusses the alleged use of Internet communication in Osama bin Laden's order to bomb two U.S. embassies, send his alleged commands through encrypted messages, and study terrorist tactics on the Internet. At least one lawmaker, according to this article, cited the bombings as reason for controlling encryption. The FBI has long argued that unrestricted exports of encryption would give criminals a new way to cover their tracks. This article brings up the argument

---

<sup>39</sup> Justin Matlick, *U.S. Encryption Policy: A Free-Market Primer* (visited Mar. 13, 2000) <<http://www.pacificresearch.org>>.

<sup>40</sup> Courtney Macavinta, *Terrorism Plays into Net Debate* (visited Mar. 13, 2000) <<http://news.cnet.com/news/>>.

that U.S. software makers and privacy advocates use to counter that concern – that the technology is already available around the world and that the Clinton administration regulations only inhibit American firms' ability to ship the products that are most in demand.

The NSA has also been vocal about the need to limit the spread of encryption. They cite their charter and mission, which focuses on foreign intelligence gathering, but which may have some overlap into domestic surveillance. To the NSA as well as the FBI, encryption poses a problem with no certain fix as criminals use the strong cryptographic technologies to hide their crimes.<sup>41</sup>

Attorney General Janet Reno saw the need to restrict use and dissemination of encryption over the Internet, and in fact went to far as to suggest the ban of such encryption distribution.<sup>42</sup> In a letter to the German Federal Secretary of Justice, Reno announced her concerns about nations not limiting the intangible export of strong encryption, and the effect this would have of making international encryption controls illusory. Thus law enforcement officials have sought not only to control encryption in the United States, but worldwide.

### **Encryption as a Munition**

Many reports on encryption begin with legislative background behind ITAR.<sup>43</sup> The AECA statute allowed the creation of regulations to control the import and

---

<sup>41</sup> William Cohen et al., *Preserving America's Privacy and Security in the Next Century: A Strategy For America In Cyberspace: A Report to the President of the United States* (last modified Sep. 16, 1999) <[www.Cdt.Org/Crypto/CESA/Cesawhitepaper.Shtml](http://www.Cdt.Org/Crypto/CESA/Cesawhitepaper.Shtml)>.

<sup>42</sup> See Reno Calls for Ban on Encryption Products on the Net, Newbytes PM, July 28, 1999, available in LEXIS, News Library, Asapii File.

<sup>43</sup> See, e.g., David Loundy, *Try Decoding The Latest In Munitions-Wear*, CHI. DAILY L. BULL., Sept. 14, 1995, at 6.

export of designated defense articles and services found on the munitions list.<sup>44</sup> These regulations were ITAR, of which the munitions list is one part, and one item on the munitions list is cryptographic software. Specifically, “components or software with the capability of maintaining secrecy or confidentiality of information or information systems.”<sup>45</sup> Because it was on the list, the law prohibited exporting cryptographic software (or technical data about cryptographic software) without a license from the U.S. Department of State. Included in this definition of “export” was disclosing or transferring technical data to a foreign person, either in the U.S. or abroad.

At the end of 1996, Clinton transferred oversight from the Department of State to the Department of Commerce, where cryptography export fell under the Export Administration Regulations<sup>46</sup> (EARs) and was overseen by the Bureau of Export Administration.<sup>47</sup>

After the transfer of encryption, there were ongoing attempts during the Clinton years to resolve encryption issues.<sup>48</sup> At the time of the article, three bills had been introduced in Congress that would liberalize export restrictions and derail some Clinton administration attempts to guarantee access to encrypted communications. The basic issue presented was how the law should be updated to account for changes in technology and the political environment. The paper suggested electronic commerce and the security of electronic messages rely on encryption. Traditionally,

---

<sup>44</sup> U.S. Munitions List (22 C.F.R. §§ 121.1-.15).

<sup>45</sup> *Id.*

<sup>46</sup> Rules governing exports of encryption are found in the Export Administration Regulations, 15 C.F.R. Parts 730-774.

<sup>47</sup> In December 1996, President Clinton shifted licensing authority for nonmilitary encryption commodities and technologies from the State Department to the Department of Commerce. See Exec. Order No. 13,026, 61 Fed. Reg. 58,767 (1996).

<sup>48</sup> David Loundy, *Congress Scrambles To Address Encryption Issues*, CHI. DAILY L. BULL., Mar. 13, 1997, at 5.

encryption was used by spies and governments during the Cold War to keep secret plans to sink submarines and blow up embassies and the like. With this in mind, encryption hardware and software, certain technical data, and discussions of the higher mathematics that forms the basis of cryptography were treated by the U.S. as munitions. Today, much stronger forms of encryption than those which were used during the last few world wars are used to protect the \$5 smart-card used to buy a Slurpee at the local 7-11. However, the law had not changed in order to match the evolving role of the technology, or the environment in which that technology is used.

### **Military Uses of Encryption**

A critical aspect of the evolution of encryption regulation focuses on the protection of military computer systems from Internet threats.<sup>49</sup> When the military was initially exploring the possibility of connecting defense-related systems to the Internet to support global communications requirements, before taking that step, there were many risks and security issues to be understood. Safeguards and procedures needed to be implemented to ensure that national security information did not end up in the wrong hands. To achieve an open systems environment, the military often uses such commercial software in its computer and communications systems, which therefore exposed them to the same risks as everyone else. To prevent unauthorized access to protected computer and communications systems and to improve overall information security, there were a number of precautions to be taken at the host and network levels. For instance, information could be encrypted when it is transmitted

---

<sup>49</sup> *Protecting Military Computer Networks From Internet Threats* (visited Mar. 13, 2000) <<http://www.telos.com/corpinfo/feature/infosec/abstract.html>>.

across the Internet which would prevent it from being read by unauthorized individuals in the event it was intercepted. Additionally, encryption could be used to protect sensitive information while it resides on a computer.<sup>50</sup>

An important point made early in the paper is that despite the DoD's leadership role in information security, the DoD would have to expand its focus if defense systems were connected to the Internet. That is, *the DoD would have to take the same precautions as commercial organizations that conduct business over the Internet*. It is important for the U.S. government to leverage Internet security advancements made in the commercial sector to maintain security of DoD systems that were to connect to the information superhighway.

These ideas supported the concept of allowing commercial encryption technology to advance as much as possible, and should have acted as a counter to arguments that national security depends on limiting strong encryption's use and development in the United States. Instead conflicting ideas are apparent. Federal agencies should have the strongest encryption available to protect their communication and infrastructure, but that its use, dissemination, development within the United States should be curtailed and discouraged.

## **Privacy Issues**

Privacy has become a central issue throughout the different attempts at encryption legislation in the United States.<sup>51</sup> Federal information-gathering systems

---

<sup>50</sup> *Id.*

<sup>51</sup> *See, e.g.,* Solveig Singleton, Privacy Issues in Federal Systems: A Constitutional Perspective, Remarks before the National Institute of Standards and Technology Computer System Security and Privacy Advisory Board Meeting (Mar. 17, 1999).

raise similar concerns about privacy and Fourth Amendment search and seizure violations. The range of concerns includes danger to human rights from federal information systems, security concerns such as identity theft, and the role of encryption in federal systems. Privacy in federal systems is an important component of protecting against threats to human rights, especially because it is not unknown for federal agencies and employees to use information stored in federal systems to carry on personal or political vendettas, or violations of rights on a grander scale.

Many reports completed in the past several years have touched on the issues of wiretapping and the Electronic Communications Privacy Act (ECPA).<sup>52</sup> The ECPA is part of the U.S. Criminal Code that generally forbids the use of wiretaps without some form of court order, either a full Title III (probable cause-based) court order for obtaining communications' content or an ECPA-created court order based upon relevancy for communications' addressing and transactional record information.<sup>53</sup> In addition, the act prohibits disclosure of the contents of an electronic communication to any person or entity unless certain requirements are met. Of course, there are still the "emergency" provisions whereby surveillance is permitted to proceed immediately, when high-level Department of Justice authorization is obtained, so long as a court order is filed within 48 hours.

This act in 1986 was the last electronic privacy law enacted, which causes concern among privacy activists in light of rapidly changing technology. The fear is, again, that U.S. law just is not responding to changes in technology, the more intrusive nature of evolving law enforcement surveillance technologies, and threats to

---

<sup>52</sup> 18 U.S.C. §§ 2701-2711.

<sup>53</sup> *Carnivore Diagnostic Tool*, *supra* note 34.

privacy and unrestricted speech. With no certainty of secure communication, the specter of “Big Brother” and self-censorship looms large.

### **Historical Perspectives**

Simon Singh’s “The Code Book” offers an exploration of historical uses of cryptography, extending up to current use of digital encryption systems.<sup>54</sup> The book details ancient history, describing people using some form of encoded messages and secret communication back as far back as the feud between Greece and Persia.<sup>55</sup> Singh talks about the emergence of the telegraph and the concurrent use of Morse Code, which he said together had an increasing influence on the world, enabling the police to capture more criminals, helping newspapers to bring the very latest news, providing valuable information for businesses, and allowing distant companies to make instantaneous deals. Singh points out that even then, guarding these often sensitive communications was a major concern. The telegraph operators had access to every message, and hence there was a risk that one company might bribe an operator in order to gain access to a rival’s communications.<sup>56</sup> This risk can be seen as a simplified precursor to today’s national security risks.

The development of the telegraph drove the commercial interest in cryptography and generated public interest in cryptography. The public became aware of the need or desire to protect personal messages of a highly sensitive nature, and if necessary people would use encryption. The ciphers used by the general public

---

<sup>54</sup> SIMON SINGH, THE CODE BOOK (1999).

<sup>55</sup> *Id.* at 4.

<sup>56</sup> *Id.* at 61.

would not have withstood attack by a professional cryptanalyst, but they were sufficient to guard against the casual snooper.

The introduction of radio communication was also an important landmark, which proved of interest to the military. The tactical advantages of radio were apparent, allowing direct communication between any two points without the need of a wire between the locations. However, this all-pervasive property of radio was also its greatest military weakness, because messages could reach the enemy as well as the intended recipient. Consequently, reliable encryption became a necessity. Singh says this became especially apparent during World War I.

There were also more mundane public uses of cryptography, such as the cipher disc. Even though the cipher disc was a very basic device, it made encipherment easier, and it endured for five centuries. One example was the Code-o-Graph, a cipher disc used by the hero of Captain Midnight, one of the early American radio dramas. Listeners could obtain their own Code-O-Graph by writing to the program sponsors. Occasionally the program would end with a “secret message” from Captain Midnight, which could be deciphered by loyal listeners using the Code-o-Graph.<sup>57</sup>

Finally, the evolution approaches the use of computers in communication. During the 1960s, computers became more powerful, and at the same time they became cheaper. Businesses were increasingly able to afford computers, and could use them to encrypt important communications such as money transfers or delicate trade negotiations. However, as more and more businesses bought computers, and as use of encryption by and between businesses spread, cryptographers were confronted

with new problems, difficulties that had not existed when cryptography was solely in the hands of governments and the military. One of the primary concerns was the issue of standardization. A company might use a particular encryption system to ensure secret internal communication, but it could not send a secret message to an outside organization unless the receiver used the same system of encryption. It is a short journey to the now-familiar concepts of the privacy versus national security issues of encryption use on the Internet.

### **Research Questions**

Much of the research discussed above focused on the evolving encryption regulations which for so long failed to take into account the history of encryption use as a military and National Security Agency tool, and encryption's subsequent entrance into the public and private spheres. Regulation was used as a direct control to isolate the Internet as a form of communication and target it in ways that would never be allowed in other media. The controls in place and suggested are overly intrusive without showing adequate justification for being so, and affront current notions of First Amendment and privacy rights.

This thesis explains the evolution of encryption from military to private use, the failure of government regulations to recognize and adapt to that change, and the subsequent specialized treatment of Internet communication. The main purposes of this thesis were to discover why the government is pursuing regulation and limitations on communication over the Internet (e.g., to maintain control over private and corporate uses and exportation of strong encryption) so differently than

---

<sup>57</sup> *Id.* at 124.

communication through more traditional media; to argue that government intervention into private and business uses of the Internet for communication are overly intrusive, treading on citizens' rights; and that such regulations belong in the military and National Security Agency realms only. The research then, will focus on the question of should the Department of Defense and military regulations be imposed on civilian encryption and Internet users? To answer this question, it will be necessary also to examine whether the current regulations reflect the changing nature of encryption and Internet technology, and how the regulations promulgated during the Clinton administration conflict with citizens' rights.

### **Methodology**

The primary methodology to be used for this thesis will be legal and historical methods. This will included legal research of rulings regarding message and information transfer on the Internet, censorship on the Internet, and Internet regulations and rules in general. Three main cases will be the focus of free speech issues as directly confronted by the encryption regulations. Other legal research included court rulings on privacy over the Internet, and research into cases on privacy in communications over other media. It will also be necessary to research violations of First and Fourth Amendment and privacy rights as they apply to the Internet.

Much of the research was targeted at a review of the Clinton administration initiatives, and the evolution of those regulations. The effects of both national and international policies on domestic and international encryption use will be addressed.

Further to this, there will be an examination other government monitoring abilities and the regulations, limitations and infrastructure which support those schemes.

There will also be historical research into encryption or encoding over other media (e.g. cryptography in media other than the Internet) and the evolution of cryptography itself, including DoD and NSA regulations of the same. This historical research will include a study of cases of the difference between media significantly resulting in a difference in regulation of messages. The cutoff for research will be December 31, 2000.

## CHAPTER 3

### HISTORY OF THE MILITARY, NSA, AND THE INTERNET

#### History in Wartime

When studying encryption regulations, it is important to note that this technology has been characterized by government and military involvement since its inception. Before there was computer encryption, there were other kinds of cryptography, also of vast importance during wartime situations. Cryptography is defined as the science, or art, of secret writing. The term “cryptography” itself comes from two Greek words, *Crypto*, meaning *hidden*, and *Graphia*, *writing*. References are made to cryptography in the bible. Early cryptographic systems are known to have existed in the days of Julius Caesar. One such system, referred to as the Caesar Cipher, replaced each letter of an encrypted message with the letter three places beyond it in the regular alphabet.<sup>58</sup> Throughout history cryptography has played an important role whenever there has been a need to conceal the meaning of messages, particularly with espionage during wartime.

Encryption can be defined as the translation of data into a secret code, and is one of the most effective way to achieve data security. To read an encrypted file, the reader must have access to a secret key or password that enables decryption. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

---

<sup>58</sup> Huffman et al., *supra* note 21.

There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption.<sup>59</sup> Symmetric encryption is type of encryption in which the same key is used to encrypt and decrypt the message.<sup>60</sup>

Public-key encryption is a cryptographic system that uses two keys – a *public key* known to everyone and a *private* or *secret key* known only to the recipient of the message. When someone wants to send a secure message to the receiver, the sender uses the receiver's public key to encrypt the message. The recipient then uses the private key to decrypt it. An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key by only knowing the public key.<sup>61</sup>

Foreign agents, both in the U.S. and abroad, used cryptography extensively for decades. Encryption devices such as the mechanical Enigma machine and its counterparts, which were used to encode and decode messages during the second World War, were popular until they were rendered obsolete by both technology and cryptographers who figured out how to break Enigma-encoded messages. In the past, the use of cryptography was limited. The players, primarily government entities, were involved in the relatively exclusive, top-secret business of sending, receiving and attempting to intercept and decode the messages of others.<sup>62</sup>

---

<sup>59</sup> *Encryption* (visited Mar. 12, 2000)

<<http://webopedia.internet.com/Networks/Security/Encryption/encryption.html>>.

<sup>60</sup> *Symmetric key* (visited Mar. 12, 2000)

<[http://webopedia.internet.com/TERM/s/symmetric\\_key\\_cryptography.html](http://webopedia.internet.com/TERM/s/symmetric_key_cryptography.html)>.

<sup>61</sup> *Public key cryptography* (visited Mar. 12, 2000)

<[http://webopedia.internet.com/Networks/Security/Encryption/public\\_key\\_cryptography.html](http://webopedia.internet.com/Networks/Security/Encryption/public_key_cryptography.html)>.

<sup>62</sup> Huffman et al., *supra* note 21.

With the growth of the Internet, many new cryptographic players have emerged, such as banks, corporations, organizations, and individuals with access to sophisticated technology who are sending and receiving large amounts of often highly sensitive information on the Internet, which is itself primarily an unsecured public network. Everything from multi-billion dollar financial transactions and personal medical information to credit card numbers and criminal histories is being transmitted on the Internet.<sup>63</sup>

### **NSA uses of Cryptography**

The National Security Agency (NSA) is another entity which has historically made extensive use of cryptography. The NSA performs electronic surveillance to collect foreign intelligence information for the military and policymakers. The NSA provides valuable intelligence to U.S. government consumers on a wide range of issues of concern to all Americans, such as international terrorism, narcotics trafficking, and proliferation of weapons of mass destruction. NSA's electronic surveillance activities are subject to strict regulation by statute<sup>64</sup> and Executive Order<sup>65</sup> due to the potential intrusiveness and the implications for the privacy of U.S. persons<sup>66</sup> of these activities.

NSA's electronic surveillance authority is found in Executive Order 12333, entitled "Intelligence Activities." Executive Order 12333 authorizes NSA to collect, process, and disseminate signals intelligence information for national foreign

---

<sup>63</sup> Huffman et al., *supra* note 21.

<sup>64</sup> The Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 et seq.

<sup>65</sup> Exec. Order No. 12333, 3 C.F.R. 200 (1982), reprinted in 50 U.S.C. § 401 note.

intelligence (and counterintelligence) purposes and in support of U.S. military operations.<sup>67</sup> NSA is authorized to collect information only for foreign intelligence purposes and to provide it only to authorized government recipients.<sup>68</sup>

A memorandum from President Truman established NSA in 1952 stated that “the communications intelligence activities of the United States are a national responsibility.”<sup>69</sup> NSA’s charter, a Department of Defense document, creates “a unified organization structured to provide for the signals intelligence (SIGINT) mission of the United States and to insure secure communications systems for all departments and agencies of the U.S. government.”<sup>70</sup>

One example of NSA’s success in their communication intelligence, specifically cryptanalysis, is the VENONA Project – a program to examine and if possible, exploit encrypted Soviet diplomatic communications. Three years after a 1944 cryptanalytic breakthrough, Meredith Gardner, one of the VENONA analysts, was able to read two KGB messages revealing that someone inside the War Department general staff was providing highly classified information to the Soviets.<sup>71</sup>

---

<sup>66</sup> “U.S. persons” is a term which includes citizens, permanent resident aliens, groups substantially composed of either or both of these categories of individuals, and corporations incorporated in the United States.

<sup>67</sup> See 50 U.S.C. § 1801(i) and E.O. 12333, § 3.4(i). See *Id.* at § 1.12(b)(3), (4), (5), (6), and (7). Signals intelligence is comprised of communications intelligence and electronics intelligence. Communications intelligence consists of foreign communications passed by radio, wire, or other electromagnetic means and electronics intelligence consists of foreign electromagnetic radiations such as emissions from a radar system.

<sup>68</sup> *Testimony Before the House Permanent Select Committee on Intelligence*, 106th Cong. (2000) (statement of Lt. Gen. Michael V. Hayden, USAF, Director, National Security Agency).

<sup>69</sup> NSA established in the Department of Defense by National Security Council Intelligence Directive No. 9, December 29, 1952, under authority of a Presidential memorandum, October 29, 1952, effective November 4, 1952.

<sup>70</sup> NSA surveillance authority is found in Exec. Order No. 12333, 3 C.F.R. 200 (1982), reprinted in 50 U.S.C. § 401 note.

<sup>71</sup> Lt. Gen. Michael V. Hayden, Address at the Kennedy Political Union of American University (Feb. 17, 2000).

VENONA translations pointed to over 200 named or covernamed persons then present in the U.S. claimed by KGB and soviet military intelligence messages as clandestine assets or contacts. The messages disclose some of the clandestine activities of Julius and Ethel Rosenberg, Harry Gold, Klaus Fuchs, David and Ruth Greenglass, and others involved with atomic bomb espionage.<sup>72</sup>

As early as 1960, American intercept operators began hearing Spanish along with the usual Slavic languages coming from airfields in Czechoslovakia. As for the importance of the NSA mission to national decision making, its signals intelligence played a significant role in managing the Cuban Missile Crisis. NSA collected early indications of the arms buildup beginning in Cuba, exploiting Soviet communications concerning ships headed to Havana—ships whose cargo manifests were suspiciously blank.

According to NSA Director Lt. Gen. Michael V. Hayden, the founding principles of SIGINT helped the United States to win the Cold War.<sup>73</sup> Funding, in light of the clear, ongoing threat to America, was vigorous and consistent. But today, the NSA is an agency in change. In this new era, the global environment is no longer defined using a map.<sup>74</sup> Twenty years ago, few people outside of government or research used a computer—much less had one at home. Forty years ago there were 5,000 stand-alone computers, no fax machines and not one cellular phone. Today, there are over 180 million computers -- most of them networked. There are roughly 14 million fax machines and 40 million cell phones and those numbers continue to

---

<sup>72</sup> *Id.*

<sup>73</sup> *Id.*

<sup>74</sup> Hayden, *supra* note 68.

grow. These factors all contribute to the changing way of business for the NSA, and the increase in challenges it faces.<sup>75</sup>

## **NSA, DoD Regulations**

The military and government uses of encryption over the Internet extend back in more than one direction. Not only has the Department of Defense been a user of such technology, but in the area of the Internet, it was one of the driving factors in encryption's development. The Defense Advanced Research Projects Agency (DARPA) is the central research and development organization for the Department of Defense. It manages and directs selected basic and applied research and development projects for DoD, and pursues research and technology where risk and payoff are both very high and where success may provide dramatic advances for traditional military roles and missions and dual-use applications.<sup>76</sup> DARPA's early initiatives, the advent of ARPANET and the subsequent proliferation of the Internet and the world wide web – all these have forged the way for a brave new world for encryption uses.

In 1957, President Dwight D. Eisenhower first saw the need for the Advanced Research Projects Agency (ARPA)<sup>77</sup> after the Soviet Union's 1957 launch of *Sputnik*. The organization united some of America's most brilliant people, who developed the United States' first successful satellite in 18 months. Several years later ARPA began to focus on computer networking and communications technology. In 1962, Dr. J.C.R. Licklider was chosen to head ARPA's research in improving the

---

<sup>75</sup> Hayden, *supra* note 71.

<sup>76</sup> *Defense Advanced Research Projects Agency* (visited Feb. 25, 2000) <<http://www.darpa.mil/>>.

<sup>77</sup> The Advanced Research Projects Agency (ARPA) changed its name to Defense Advanced Research Projects Agency (DARPA) in 1971, then back to ARPA in 1993, and back to DARPA in 1996.

military's use of computer technology. Licklider was a visionary who sought to make the government's use of computers more interactive. To quickly expand technology, Licklider saw the need to move ARPA's contracts from the private sector to universities and laid the foundations for what would become the ARPANET.<sup>78</sup>

The point that I do want to dust off and raise again is that ARPA wouldn't have happened, if what used to be the Soviet Union hadn't shaken complacent U.S. awake with a tin can in the sky, *Sputnik*. Wars do wonders for the advancement of technology, and the Cold one was certainly no exception. The way to get a technology advanced is to gather a lot of really smart people under one roof and get them to concentrate on a single project. Of course, that takes some organization and money. In this case, it was the only body that had a stake in making sure the Net worked - the government.

What with the Cold War in full swing and all, the military...was concerned that if the war ever got hot and large chunks of the country were vaporized, those phone lines (not to mention considerable segments of the population) would be radioactive dust. And the top brass wouldn't be able to get in touch and carry on. Thus the packets bouncing from node to node, each of those nodes able to send, receive and pass on data with the same authority as any other. It was anarchy that worked....<sup>79</sup>

## The ARPANET

In 1973, DARPA initiated a research program to investigate techniques and technologies for interlinking packet networks of various kinds. The objective was to develop communication protocols which would allow networked computers to communicate transparently across multiple, linked packet networks. This was called the Internetting Project and the system of networks which emerged from the research was known as the "Internet." The system of protocols which was developed over the course of this research effort became known as the TCP/IP Protocol Suite, after the

---

<sup>78</sup> Gregory R. Gromov, *History of Internet and WWW: The Roads and Crossroads of Internet History* (visited Feb. 24, 2000) <<http://www.Internetvalley.com/intval.html>>.

two initial protocols developed: Transmission Control Protocol (TCP) and Internet Protocol (IP).

A great deal of support for the Internet community has come from the U.S. federal government, since the Internet was originally part of a federally-funded research program and, subsequently, has become a major part of the U.S. research infrastructure. During the late 1980's, however, the population of Internet users and network constituents expanded internationally and began to include commercial facilities. Indeed, the bulk of the system today is made up of private networking facilities in educational and research institutions, businesses, and government organizations across the globe.<sup>80</sup>

### **How Encryption Works**

Modern encryption is achieved with algorithms that use a “key” to encrypt and decrypt messages by turning text or other data into digital gibberish and then by restoring it to its original form. The longer the key, the more computing required to crack the code. To decipher an encrypted message by brute force, one would need to try every possible key. Computer keys are made of “bits” of information, binary units of information that can have the value of zero or one. So an eight-bit key has 256 (2 to the eighth power) possible values. A 56-bit key creates 72 quadrillion possible combinations.<sup>81</sup>

---

<sup>79</sup> David Hudson, *Journal of a Strained Net* (last modified Aug 9, 1996)  
<<http://www.Internetvalley.com/intval.html>>.

<sup>80</sup> *A Brief History of the Internet and Related Networks* (visited Feb. 25, 2000)  
<<http://www.isoc.org/Internet/history/cerf.html>>.

<sup>81</sup> Amy Branson and Dan Froomkin, *Deciphering Encryption* (last modified May 8, 1998)  
<[www.washingtonpost.com/wp-srv/politics/special/encryption/keystories.htm](http://www.washingtonpost.com/wp-srv/politics/special/encryption/keystories.htm)>.

If the key is 128 bits long, or the equivalent of a 16-character message on a personal computer, a brute-force attack would be 4.7 sextillion (4,700,000,000,000,000,000,000) times more difficult than cracking a 56-bit key. Given the current power of computers, a 56-bit key is considered crackable; a 128-bit key is not – at least not without an enormous amount of effort.

Until 1996, the U.S. government considered anything stronger than 40-bit encryption a “munition” and its export, therefore, was illegal. Even as the government moved to allow the export of 56-bit encryption, with some restrictions, the fast pace of changing technology had 128-bit cryptography emerging as the new digital standard.<sup>82</sup>

### **A Flourishing Internet**

Widespread development of local area networks (LANs), personal computers, and workstations in the 1980s allowed the budding Internet to flourish. At the same time that the Internet technology was being experimentally validated and widely used amongst a subset of computer science researchers, other networks and networking technologies were being pursued.<sup>83</sup> The usefulness of computer networking - especially electronic mail - demonstrated by DARPA and Department of Defense contractors on the ARPANET was not lost on other communities and disciplines, so that by the mid-1970s computer networks had begun to spring up wherever funding could be found for the purpose.

---

<sup>82</sup> *Id.*

<sup>83</sup> Vinton Cerf, et al., *A Brief History of the Internet* (visited Feb. 24, 2000) <<http://www.isoc.org/Internet/history/brief.html>>.

One should not conclude that the Internet has now finished changing. The Internet, although a network in name and geography, is a creature of the computer, not the traditional network of the telephone or television industry.<sup>84</sup> It will continue to change and evolve at the speed of the computer industry if it is to remain relevant. It is now changing to provide such new services as real time transport, in order to support, for example, audio and video streams. The availability of pervasive networking (the Internet) along with powerful affordable computing and communications in portable form (laptop computers, two-way pagers, cellular phones), is making possible a new paradigm of nomadic computing and communications.<sup>85</sup>

This evolution resulted in new applications, such as more sophisticated forms of pricing and cost recovery, and yet another generation of underlying network technologies with different characteristics and requirements, from broadband residential access to satellites. New modes of access and new forms of service will spawn new applications, including more sophisticated means of keeping data secure, which in turn will drive further evolution of the net itself.<sup>86</sup>

With the growth of the Internet came the proliferation of encryption, and the U.S. government, through agencies like the NSA and FBI, realized that it no longer had a monopoly on the use of cryptography. Unless steps were taken to protect the government's ability to intercept and decode digital, encrypted communications, the government felt the security of its own communications and national security would be placed in jeopardy. Government and law enforcement would lose some of its

---

<sup>84</sup> *Id.*

<sup>85</sup> *Id.*

ability to fight crime and terrorism, and the integrity of vital communications, including those needed to maintain public infrastructures such as power and the switched public telecommunications network, might be subject to compromise. It was inevitable that the different interests would clash, particularly as public concern about privacy continued to grow in the 1990s.<sup>87</sup>

Before 1991, the government and large companies were still the only real users of encryption technology. That began to change when programmer Philip Zimmermann released free software called Pretty Good Privacy, which encodes ordinary e-mail. Its domestic use was never challenged. But when PGP turned up in other countries, the Department of Justice launched a three-year criminal investigation of Zimmermann. PGP used 128-bit encoding keys at a time when U.S. export laws allowed only 40-bit encryption to cross the borders. Anything stronger was classified a munition, just like guns and warheads.<sup>88</sup>

### **Foundation of Encryption Regulations**

In 1995, 28 countries decided to establish the *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*.<sup>89</sup> The Wassenaar Arrangement controls the export of weapons and of dual-use goods – goods that can be used both for a military and for a civil purpose; cryptography is such a dual-use good. Cryptography export used to be controlled by ITAR,<sup>90</sup> which

---

<sup>86</sup> *Id.*

<sup>87</sup> Huffman et al., *supra* note 21.

<sup>88</sup> Branson, *supra* note 81.

<sup>89</sup> Bert-Jaap Koops, *Crypto Law Survey: Version 17.0, February 2000* (visited May 4, 2000) <<http://cwis.kub.nl/~frw/people/koops/lawsurvey.htm>>.

<sup>90</sup> International Traffic in Arms Regulations, 22 C.F.R. pts. 120-130 (1995).

restricted export of “dual-use” goods. The arrangement received final approval by 33 co-founding countries in July 1996 and began operations in September 1996.

At the end of 1996, in the United States cryptography export was transferred to the EARs<sup>91</sup> of the Department of Commerce. The Department of Commerce classified the posting of encryption material on the Internet as an “export” because foreigners could easily access the material. The regulations went so far as to prohibit professors from lecturing on encryption when they are aware of foreigners in their audience.<sup>92</sup> However, the regulations define “export” to include simple publication in the U.S., as well as discussions with foreigners inside the U.S.<sup>93</sup> They also defined “software” to include printed English-language descriptions and diagrams, as well as the traditional machine-readable object code and human-readable source code. Another provision in the Arms Export Control Act said that export control decisions were not subject to judicial review (under the Administrative Procedures Act).<sup>94</sup>

Part of the government’s requirements are that someone seeking to “export” encryption register as an arms dealer and seek government permission before publication. This is required by the Arms Export Control Act and its implementing regulations, the International Traffic in Arms Regulations.<sup>95</sup> This specification has been the focus of the Bernstein,<sup>96</sup> Karn,<sup>97</sup> and Junger,<sup>98</sup> cases which have challenged the regulations.

---

<sup>91</sup> Rules governing exports of encryption are found in the Export Administration Regulations, 15 C.F.R. Parts 730-774.

<sup>92</sup> *Junger v. Daley*, 8 F. Supp. 2d 708 (N.D. Ohio 1998).

<sup>93</sup> See Bert-Jaap Koops, *supra* note 89.

<sup>94</sup> Administrative Procedure Act (APA), 5 U.S.C. § 706(2) (a).

<sup>95</sup> *Court Declares Crypto Restrictions Unconstitutional: Free Speech Trumps Clinton Wiretap Plan* (last modified Dec. 19, 1996) <[www.eff.org](http://www.eff.org)>.

<sup>96</sup> *Bernstein v. Department of State*, 922 F. Supp. 1426 (N.D. Cal. 1996) (*Bernstein I*).

<sup>97</sup> *Karn v. U.S. Department of State*, 925 F.Supp. 1 (D.D.C. 1996).

The U.S. government, both the Department of Defense and the military, as well as agencies such as the NSA, have long been involved with developing, using, and controlling cryptography and computer encryption as valuable tools for maintaining national security. This is an invaluable starting point to keep in mind when examining other encryption uses, and the regulations that concern them, that have evolved over the years.

---

<sup>98</sup> *Junger v. Daley*, 8 F. Supp. 2d 708 (N.D. Ohio 1998).

## CHAPTER 4

### FEDERAL AND MILITARY ENCRYPTION REGULATION

As discussed in Chapter 2, cryptography as it evolved was primarily used by the military and defense organizations such as the NSA and FBI, concerned with intelligence and counterintelligence activities. As such, and as with any process important to national security, a series of U.S. Department of Defense regulations evolved. These concern classification, use, transfer, and sharing of sensitive material, as well as outlining stiff penalties for abuse, misuse, mishandling, or compromise of such information.

The military and the NSA both have a fixed and known dependence on access to and the careful control of information. The NSA mission has always focused on foreign, or international, intelligence, although it may sometimes coincidentally overlap with some domestic intelligence activities. They both also maintain regulations on handling of such information, which are necessary to ensure the integrity of the system.

Also mentioned in Chapter 2, although there was some commercial and private use of encoding information, these codes were generally less advanced, and would not have stood up to serious, professional decryption attempts. In general, these were used mainly to protect private information from casual or inexperienced attempts. So until recently, encryption was relegated to the realm of national security.

President Truman's 1952 memorandum made it clear that communications intelligence is a national responsibility. The NSA mission to insure secure

communications systems for all departments and agencies of the U.S. government<sup>99</sup> was and is clearly important, but its newest charter and founding documents were made many years ago. The most recent founding document is an executive order issued by President Reagan in 1982<sup>100</sup> which reaffirmed both the importance of intelligence and the principles guiding its collection.<sup>101</sup> The NSA role is not just to acquire information, but also to protect it, especially where national security information is concerned.<sup>102</sup>

### **DoD and Military Regulations**

The DoD has regulations and handbooks specifically for dealing with classified and encrypted material, as do each of the United States military services. The U.S. Air Force regulations will serve to illustrate the nature and scope of military publications on the subject.

First, a brief example of some of the DOD publications.

DoD 5200.1-H	Department of Defense Handbook for Writing Security Classification Guidance (November 99)
DoD 5200.1-R	Information Security Program (January 1997)
DoD 5220.22-S	COMSEC Supplement to Industrial Security Manual for Safeguarding Classified Information (March 1988)

DoD 5200.1-R, The Information Security Program, specifically relates to classified national security information, and to demonstrate its wide range, it applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the

---

<sup>99</sup> Hayden, *supra* note 71.

<sup>100</sup> Exec. Order No. 12333, 3 C.F.R. 200 (1982), reprinted in 50 U.S.C. § 401 note.

<sup>101</sup> *See id.*

<sup>102</sup> *See id.*

Department of Defense, the Uniformed Services University of the Health Sciences, the Defense Agencies, and the DoD Field Activities.

The COMSEC supplement to the Industrial Security Manual for Safeguarding Classified Information, establishes uniform security practices within facilities used by prime and sub-contractors having custody of classified or unclassified COMSEC equipment/material of the DoD and certain other executive departments and agencies. This regulation also makes a point of its coordination with the NSA in dealing with “provisions relative to Controlled Cryptographic Items.” These provisions delineate minimum requirements for the acquisition and ownership, transportation, physical security and access control, key accounting, reporting of insecurities, and disposition of CCI materials at contractor facilities.

There are many Air Force regulations on classification of material and handling of secure information, many of which are themselves classified and not available to the general public. Those which are available include, among others:

AFI 33-210 (19 May 2000)	Cryptographic Access Program
AFI 31-401 (1 January 1999)	Information Security Program
	Management
AFI 33-216 (1 November 1997)	Management of Manual Cryptosystems
AFPD 31-4 (1 September 1998)	Information Security
AFPD 61-2 (7 April 1993)	Management Of Scientific and Technical
	Information
AFPD 71-1 (1 July 1999)	Criminal Investigations and
	Counterintelligence

AFI 33-210 specifies the minimum qualifications for military personnel to qualify for access to cryptographic material, including that they hold U.S. citizenship; be a DoD civilian employee, a DoD-cleared contractor or contractor employee, or a military servicemember; have a final security clearance and security investigation

appropriate to the classified cryptographic information level accessed; receive a security briefing detailing the sensitive nature of cryptographic material and the individual's responsibility to protect cryptographic material; and consent to periodic counterintelligence security polygraph examinations. Polygraph examinations encompass only questions concerning disloyal activities, espionage, sabotage, terrorism, and general honesty and trustworthiness.

The briefing servicemembers must receive before even having access to classified material includes the statements that the member must understand "the safeguards that protect this information, the directives that govern authorized access, and the penalties you will incur for the unauthorized disclosure, unauthorized retention, or negligent handling of U.S. classified cryptographic information."<sup>103</sup> There is also warning that failure to properly safeguard this information could cause damage or irreparable injury to the national security of the United States, and that if the servicemember willfully or negligently discloses U.S. classified information to any unauthorized persons, they will be subject to administrative and civil sanctions, as well as criminal sanctions under the Uniform Code of Military Justice and the criminal laws of the United States.

It would certainly seem apparent that given the rigorous regulations surrounding NSA, DoD, and military use (and misuse) of encryption and encrypted products, that the penalties already established would be serious and clear enough to prevent those who frequently have opportunity to abuse such technologies from doing so. It would also seem clear that those who are already involved in criminal activities will not pay heed to penalties and laws no matter what their source.

## **Encryption as a Munition, and International Agreements About Export of Such Technologies**

In light of encryption's uses, and the extensive regulatory structure built up around encryption, it comes as no surprise that for decades it was deemed a munition. It was on the United States Munitions List,<sup>104</sup> along with artillery projectors; explosives, propellants, incendiary agents and their constituents; and tanks and military vehicles.

Until relatively recently, the export of cryptography was controlled in the united States by the ITAR rules.<sup>105</sup> Although designed to control military, not civilian, technology, the sudden expansion of the use of civilian cryptography has left these regulations still controlling it as though it were of purely military significance. There was also a feeling that certain branches of the U.S. government would like to keep it this way, especially apparent during the many attempts at control made during the Clinton administration, despite the overwhelming demand for civilian cryptography.<sup>106</sup>

The situation changed in December 1996, when control of civilian cryptography was removed from the ITAR regulations and put under the control of the Department of Commerce. These changed commerce regulations were unfortunately less readable than the ITAR regulations so figuring out what was allowed became more complicated. The new regulations sometimes appeared to have expanded, rather than contracted, government control over cryptography.

---

<sup>103</sup> Air Force Instruction 33-210 Cryptographic Access Program (19 May 2000), at 10.

<sup>104</sup> *U.S. Export Control Laws And Regulations* (last modified May 11, 1999) <<http://www.hq.nasa.gov/office/codei/nasaecp/Webbrfg/tsld009.htm>>.

<sup>105</sup> International Traffic in Arms Regulations, 22 C.F.R. pts. 120-130 (1995).

On July 12, 1996, a United States-led group of 33 nations adopted the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. The arrangement is, however, non-binding and each signatory agrees only to enact domestic legislation as it sees fit to give the arrangement its effect.<sup>107</sup>

Wassenaar members placed encryption items on the original List of Dual-Use Goods and Technologies (“Dual-Use Control List”). These items are considered to be “dual use” in that they can be used for both commercial and military purposes.

<sup>108</sup>Initially, the Dual-Use Control List did not place a ceiling on the strength of exported encryption products. It also did not control encryption products that were generally available or in the public domain.<sup>109</sup> Hence, while United States encryption exporters were frustrated by domestic export policies that remained more restrictive than Wassenaar, foreign manufacturers were operating in less stringent environments.<sup>110</sup>

In December 1998, Wassenaar members revised the Dual-Use Control List, implementing a maximum bit length of 64-bits on exports of mass-market encryption software.<sup>111</sup> These caps were applicable to products including web browsers, e-mail applications, electronic commerce servers, and telephone scrambling devices. Other mass-market products, such as personal computer operating systems, word

---

<sup>106</sup> University of British Columbia Theoretical Physics Homepage (visited Dec. 2, 2000) <<http://axion.physics.ubc.ca/crypt.html#LEGAL>>.

<sup>107</sup> Karim K. Shehadeh, *The Wassenaar Arrangement and Encryption Exports: An Ineffective Export Control Regime that Compromises United States' Economic Interests*, 15 AM. U. INT'L L. REV. 271 (1999).

<sup>108</sup> 15 C.F.R. pt. 772 (1999).

<sup>109</sup> ELECTRONIC PRIVACY INFORMATION CENTER, CRYPTOGRAPHY AND LIBERTY 1999: AN INTERNATIONAL SURVEY OF ENCRYPTION POLICY (1999).

<sup>110</sup> Shehadeh, *supra* note 107, at 275.

processing, and data base programs having strengths over 64-bits were subject to controls for two years.<sup>112</sup> United States administration officials announced that the revisions would level the playing field among United States and foreign manufacturers of encryption products. Unfortunately, the United States Bureau of Export Administration still controlled mass-market encryption commodities and software at the 56-bit level. As a result, however, without a binding enforcement mechanism and the lack of any implementation by the BXA, the changes gave little hope to United States exporters; foreign encryption manufacturers continued to develop more mass-market products and gain a stronger foothold in the global encryption market.<sup>113</sup>

By the end of 1999, the United States Export Administration Regulations still only permitted the unrestricted export of encryption products with up to 56-bit encryption, with some exceptions, in spite of Wassenaar allowing for up to 64-bit. Foreign software manufacturers capitalized on this policy by developing software with 128-bit encryption or higher, catering to a hungry business and civilian market. These foreign businesses flourished as the demand for maximum security in on-line transactions continued to increase.<sup>114</sup>

However, even as the Wassenaar countries put a 64-bit limit on some products, they still agreed to control certain other software, such as that used in specific sectors such as banking, insurance and health, at the 56-bit level – but without mandating key recovery systems. According to a press release from the

---

<sup>111</sup> *Id.*

<sup>112</sup> Electronic Privacy Information Center, *supra* note 109.

<sup>113</sup> Shehadeh, *supra* note 107, at 299.

<sup>114</sup> *Id.*

German Ministry of Economy, “Certain states that had initially demanded special treatment for ‘key recovery’ products have not been successful. These were seen to be the United States and United Kingdom. Thus, the export of encryption technology will remain possible without depositing keys with government agencies.”

Nevertheless, in a seemingly contradictory statement, it was made clear the restrictions would not apply to encryption products that protect intellectual property, such as digital watermarking for items like videos, cassettes and DVD disks. This exemption is seen as a concession to the entertainment industry.<sup>115</sup> This calls the entire control regime into question. While perhaps few would argue that DVDs do not pose a threat to national security, the idea that as broad an area as “entertainment” products are in some way different than software seems anomalous. While the United States and many other countries agreed that it was best to limit the use and dissemination of strong encryption by individuals and some businesses, the idea of exemptions granted to the very profitable business of entertainment worldwide shows signs of a private agenda.

In any case, the Wassenaar Arrangement and its changing requirements and limitations were more important in name than in practice. Central to Wassenaar’s ineffectiveness is its lack of an enforcement mechanism, thereby imposing no obligation on its signatories to enact domestic legislation consistent with its provisions. Again, Wassenaar is not a law or treaty but rather is designed primarily to foster the exchange of information. Another weakness is that several of the world’s

---

<sup>115</sup> Electronic Information Privacy Center, *supra* note 109.

leading encryption-exporting nations are not parties to the arrangement, including China, India, Israel, and South Africa.<sup>116</sup>

Finally, the arrangement does not require members to control the intangible export of encryption software in cyberspace.<sup>117</sup> In the United States, however, current regulations restrict the distribution of encryption software via the Internet.<sup>118</sup> These regulations were unrealistic even when they were first set out, especially in face of the fact that people living both in and outside the United States have been able to visit the international "Pretty Good Privacy" web site and download 128-bit encryption in less than one minute.<sup>119</sup>

---

<sup>116</sup> Shehadeh, *supra* note 107, at 298.

<sup>117</sup> Encryption software that can be downloaded off the Internet is considered intangible export.

<sup>118</sup> Shehadeh, *supra* note 107, at 301.

<sup>119</sup> *PGP Downloads* (visited May 4, 2000) <<http://www.pgp.com/downloads/default.asp>>.

## CHAPTER 5

### CHANGES IN ENVIRONMENT AND ENCRYPTION REGULATION

The conjunction of encryption and national security is one of the most important issues facing our economy and society.<sup>120</sup> The implications for speech and communication in the information age cannot be stressed enough. The significant changes in the Internet environment alone should have caused a change in the fundamental basis for encryption regulation. Unfortunately, such rules, especially those mired in national security and military traditions, are difficult to change, and instead the hard and fast military and national security-based regulations were imposed – or attempted to be imposed – directly onto civilian private and commercial uses by corporations, private citizens, businesses, and schools.

Americans take it for granted that when they send a package via first class mail its contents are protected. They do not worry that someone will open their envelopes and take their checking or credit card account numbers, read their personal letters, or steal their business trade secrets or intellectual property. Yet privacy and freedom to speak without interference could be threatened as the country moves to a digital economy, where more and more information is shared electronically.<sup>121</sup>

Global efforts at regulating encryption were outlined in a 1999 report on the state of international encryption. In the United States, the FBI has several times proposed legislation that would require all manufacturers of encryption products and

---

<sup>120</sup> *Hearings on Encryption Before the Subcommittee on Telecommunications, Trade And Consumer Protection of the Committee On Commerce* (1997) (statement of George A. Keyworth II).

<sup>121</sup> *Id.*

network services to include key recovery or escrow mechanisms to enable “immediate decryption of communications or electronic information encrypted by such products or services on the public network.” At the time of the report, no new technology with encryption mechanisms would be able to be manufactured, sold, resold, distributed, or imported without the prior approval of the chief law enforcement officials of the United States. The FBI, which focuses on national issues, assisted by the NSA, which focuses on foreign intelligence issues, and the Justice and Defense Departments, have actively lobbied domestic and international organizations for encryption access programs.<sup>122</sup>

Many of these schemes not only tried to maintain national security efforts, they attempted to extend them beyond the border. One way in which the United States tried to affect international policy was through the Wassenaar Arrangement, discussed in Chapter 4. The United States was a primary architect of the 1998 changes to the Wassenaar Dual-Use Control List, although it did not succeed in its attempts to advance the concept of mandatory key recovery and extension of the dual-use list to cover intangible exports of cryptography. The export of non-military cryptographic hardware and software is still administered by the Bureau of Export Administration, a component of the Department of Commerce.<sup>123</sup>

### **Legislation Timeline**

The long-standing, though unspoken, goal of every major encryption regulation

---

<sup>122</sup> Electronic Privacy Information Center, *supra* note 109.

<sup>123</sup> *Id.*

plan by the Clinton administration was to guarantee a continuation of government access to all encrypted communications and stored data. Another goal was to keep the spread of encryption from affecting law enforcement duties and traditional surveillance capabilities. In that vein, law enforcement and national security interests have driven the process. The following is a brief history of the legislation timeline and the ongoing effort to maintain control over the changing technology of secure transmissions over the Internet.

**1993** – The Clipper Chip policy sought to achieve access through keys held by the government.

**1995** – The Clipper II proposal allowed export relief for commercial key escrow systems.

**Summer 1996** – Clipper III sought access to keys through the dual incentives of export controls and a proposal for a new government “key management infrastructure.”

**November 1996** – The Clipper 3.1.1 proposal continued to use export restrictions to enforce mandatory key escrow.

**September 1998** – The administration announced an increased bit-length allowance and granted sectoral relief to specialized industry groups.

**September 1999** – The administration announced a major reform of export controls, covering source code, retail products and posting on web sites. The final regulations were released January 2000.<sup>124</sup>

**October 2000** – The administration announced a revision to the January 2000, focusing on export to NATO and other “friendly” countries

Key to maintaining government control would be a corresponding lack of freedom of choice over encryption use in the public domain, although of course this was never publicly admitted or alluded to. This was a direct attempt to limit American citizens’ choice in the matter and a distinct curtailment of their freedom.

In an August 1995 news release, the Electronic Privacy Information Center (EPIC) reported it had obtained documents from the FBI through the Freedom of

---

<sup>124</sup> CENTER FOR DEMOCRACY AND TECHNOLOGY, AN OVERVIEW OF CLINTON ADMINISTRATION ENCRYPTION POLICY INITIATIVES (2000).

Information Act showing that the government knew years ago that initiatives such as the Clipper Chip would succeed only if other alternative security techniques and choices were outlawed.<sup>125</sup> EPIC cited a briefing document entitled “Encryption: The Threat, Applications and Potential Solutions,” endorsed by the NSA and FBI that was sent to the National Security Council in February of 1993, the time of the introduction of Clipper Chip. “Technical solutions, such as they are, will only work if they are incorporated into *all* encryption products. To ensure that this occurs, legislation mandating the use of Government-approved encryption products or adherence to Government encryption criteria is required.”

This was the point at which the government crossed the First Amendment line. What had been a maintenance of the status quo now became much more intrusive. The government’s approach to encryption, although never publicly acknowledged until recently, progressed from warrants and wiretaps to restrictions on speech through the regulation of cryptography, totally divorced from any consideration of First Amendment issues.<sup>126</sup> The government, however, continued to insist that it have “back-door” access to the programs that would allow them to decode encrypted messages.<sup>127</sup>

It is important to remember the information which individual people and businesses keep in their computer files and networks is *private*. The Clinton administration tried persistently to change the nature of that information over three or four different iterations of policy as it began to grasp that the country was entering a world of networked computing. Each of the administration policies, from the Clipper

---

<sup>125</sup> Huffman et al., *supra* note 21.

<sup>126</sup> *Id.*

Chip to mandatory key escrow to mandatory key recovery, made private information the property of the government, to some degree or other, using businesses and key managers as agents of the government. The Electronic Encryption Standard (EES) embodied in Clipper I was created with the intent of becoming a standard in government and private industry. The Clipper's encryption algorithm was classified, but could be accessed by "escrow agents" with a warrant by law enforcement to intercept the phone conversations of criminals.<sup>128</sup>

While there was some attempt to call the regimes "voluntary," it was clear that it would be difficult to avoid their use. Had government and industry actually agreed and gone through with the Clipper regime, it would have had the effect of putting the key to everyone's encryption squarely in the hands of those federal agencies who would be most tempted to use it without due process.

### **Change in Classification**

On November 15, 1996, President Clinton issued an executive order transferring jurisdiction over encryption products named as defense articles on the United States Munitions List to the Department of Commerce's Commerce Control List. Clinton included certain mass-market encryption products among the items he authorized for transfer to the CCL. The executive order *excluded* encryption products from the sections of the Export Administration Act governing controls on goods or technology that are generally available outside the United States. It was determined that the

---

<sup>127</sup> *Id.*.

<sup>128</sup> *Id.*

export of encryption products could harm national security interests – even where similar products are freely available from non-United States sources.<sup>129</sup>

Clinton's executive order, while providing key concessions to exporters, ultimately strengthened law enforcement's influence over BXA's licensing process. First, the order granted to the Department of Justice and its law enforcement bureaus greater power over the administration of export licenses. Second, the revised BXA regulations required escrow agents to meet strict eligibility standards, signaling continued commitment to create an export control policy that served the needs of law enforcement.<sup>130</sup>

However, after continued pressure from privacy activists, businesses and civil liberties organizations, on September 16, 1998, Vice President Gore announced a revised policy on encryption. The policy was changed with respect to three areas. First, it made permanent the permission to export 56-bit encryption products, although this would still be after a one-time technical review by the BXA. Second, it permitted the export of encryption products with limitless encryption capabilities to certain industrial sectors, including banking and financial institutions, on-line merchants, and health and medical organizations in all nations except those subject to United States embargoes.<sup>131</sup> Finally, the new policy expanded export opportunities by granting license exceptions for exports to such entities after a one-time technical review.<sup>132</sup>

---

<sup>129</sup> Shehadeh, *supra* note 107, at 284.

<sup>130</sup> *Id.*, at 288.

<sup>131</sup> These countries are the seven terrorist nations, including Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria.

<sup>132</sup> Shehadeh, *supra* note 107, at 290.

There were other pieces of proposed legislation in 1999 that would further signal change in the nature of encryption regulation. In early 1999, the House Judiciary Committee and House Commerce Committee endorsed legislation that would liberalize United States export control laws concerning encryption. The Security and Freedom Through Encryption (SAFE) Act<sup>133</sup> proposed to amend the Export Administration Act by removing altogether export controls on encryption products that are generally available in the public domain, or already embedded in consumer products not designed for military end-use.<sup>134</sup> Bob Goodlatte (R-Va.) argued that the proposed legislation would serve to “prevent economic crime, promote electronic commerce, and protect the personal privacy of all law-abiding Americans.” On the other hand, key congressional leaders, the Clinton administration, and law enforcement officials were opposed to the bill, saying it still compromised law enforcement and national security interests, even though it preserved the right of law enforcement officers or members of the intelligence community, acting under current law, to access encrypted communications or data.<sup>135</sup> The concern was breaking the encryption code if there were not mandatory access provisions in place.

In April 1999, Sen. John McCain (R-Ariz.) introduced a more restrictive bill, the Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act,<sup>136</sup> that would permit the export of only encryption products using key lengths of up to 64-bits. Encryption items that exceed the 64-bit threshold would

---

<sup>133</sup> H.R. 850, 106th Cong. (1999).

<sup>134</sup> Shehadeh, *supra* note 107, at 291.

<sup>135</sup> *Id.* at 292.

<sup>136</sup> S. 798, 106th Cong. (1999).

be exportable under a license exception where such products are generally or publicly available, or when a similar product using an identical or greater bit length becomes available from a foreign supplier. Moreover, the PROTECT Act authorizes export of encryption products to strategic partners of United States exporters and to members of the North Atlantic Treaty Organization, the Organization for Economic Cooperation and Development, and the Association of Southeast Asian Nations. Such exports, however, would still be subject to a license exception.<sup>137</sup>

On September 16, 1999, exactly one year after the liberalization of United States encryption export control laws, and without making SAFE or PROTECT into law, the Clinton administration announced a new series of reforms, scheduled to be implemented by December 15, 1999, and finalized and announced in January 2000. These revisions removed many regulations that United States encryption exporters deemed overly burdensome by permitting export of encryption commodities or software to businesses and other non-government end-users and mass-market encryption commodities and software of any key length, pursuant to a one-time technical review. Additionally, the administration announced that it would implement the Cryptography Note, adopted by Wassenaar members in December 1998, designed to permit the unrestricted export of mass-market encryption commodities and software with key lengths of up to 64-bits.<sup>138</sup> This began to put the United States on a more equal footing with its Wassenaar partners and other encryption developers.

---

<sup>137</sup> Shehadeh, *supra* note 107, at 295.

<sup>138</sup> *Id.*

## **Cyberspace Electronic Security Act of 1999 and Export Regulation Changes**

The government based its new regulatory scheme on three principles: a technical review of encryption products in advance of sale, a streamlined post-export reporting system, and a process that still permits the government to review exports of strong encryption to foreign governments.<sup>139</sup> In fact, in most cases a one-time product review by the export bureau continues to be required.<sup>140</sup> Companies can export commercial encryption source code to any end-user without a technical review. However, at the time of export, the exporter must submit to the BXA a copy of the source code, or a written notification of its Internet address.<sup>141</sup> Retail encryption commodities and software are those which are widely available and can be exported and reexported to anyone, and can be used to provide any product or service. However, even in these cases, it is still up to the BXA to determine which products qualify as retail through a review of their functionality, sales volume, distribution methods.<sup>142</sup>

Exports to government end-users may be approved, but these exports still are permissible only under a license. This presents no easing up of the restrictions, and is an area of wide concern about sales to governments or government-related companies. Many countries have telephone companies that are wholly or partially owned by the government, and the language in the new draft could be interpreted to

---

<sup>139</sup> Mark Grossman, *Unscrambling the Rules on Encryption*, BROWARD DAILY BUS. REV., Apr. 18, 2000, at A1.

<sup>140</sup> *Id.*

<sup>141</sup> *Id.*

<sup>142</sup> See Department of Commerce Press Release, *Administration Implements Updated Encryption Export Policy* (last modified January 12, 2000)

<<http://osecnt13.osec.doc.gov/public.nsf/docs/60D6B47456BB389F852568640078B6C0>>.

ban any sales to these companies — or to related Internet service providers.<sup>143</sup> While there were significant concessions made in the newest regulations, according to Ed Gillespie, executive director of Americans for Computer Privacy, “There remains a very complex process before anything can be exported.”<sup>144</sup>

At the same time the administration announced the new regulations, Clinton sent a legislative proposal to Congress entitled the Cyberspace Electronic Security Act of 1999 (CESA), which provides law enforcement agencies with necessary tools to combat the illegal uses of encryption. CESA authorizes the disclosure of encryption keys to recovery agents pursuant to a court order or search warrant. Under CESA, a court would grant such an order upon finding that the use of the recovery information is reasonably necessary to obtain the encrypted data, and such access is lawful, sought within a reasonable time, and does not infringe on any constitutionally protected privacy interests. While that seems sufficient on its face, exceptions to this exist in CESA under an existing “third party record” rule, where information given to a third party is deemed to lose its Fourth Amendment protection. Those cases would allow the government to obtain encryption keys or other decryption information from third parties under a court order procedure that would provide neither the probable cause nor the notice protections of the Fourth Amendment.<sup>145</sup> Another main element of CESA is its proposed authorization of appropriations to the FBI of up to \$80

---

<sup>143</sup> Adam Clayton Powell III, *New White House Cryptography Policy Criticized By Industry*, (last modified Nov. 24, 1999) <<http://www.freedomforum.org/technology/1999/11/24crypto.asp>>.

<sup>144</sup> *Id.*

<sup>145</sup> *The Fourth Amendment and the Internet, Testimony Before the Subcomm. on the Constitution of the House Judiciary Comm.*, 106th Cong. (2000) (statement by James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology).

million for a Technical Support Center that would respond “to the increasing use of encryption by criminals.”<sup>146</sup>

The most recent changes to the U.S. encryption regulations were announced in October 2000. For the most part, these revisions to the January regulations focus on further ease of exportation to the fifteen nations of the European Union and eight other countries.<sup>147</sup> While there are definite advantages to the increasingly lenient policies, there are still restrictions in place. For example, all encryption items produced by U.S. subsidiaries continue to be subject to the EARs and require review and classification before any sale or retransfer outside of the U.S. company. Many encryption commodities and software still require review and classification by the BXA. Also, licenses are still required for export to government end-users. According to the BXA press release, one of the main purposes of expanding the exportation relaxation was to create a “balanced, market-driven approach for shipping these products overseas.”<sup>148</sup> So while some still may argue that encryption policy is focused on national security issues, the evidence seems to be increasingly saying otherwise.

### **Encryption Litigation**

To date, three main cases have challenged the legality of the encryption export regulations. All were initially filed before any significant easing of policy, and while encryption was still managed under the ITAR. The principal arguments that these

---

<sup>146</sup> *Id.*

<sup>147</sup> The other countries are Australia, Japan, New Zealand, Norway, Switzerland, Czech Republic, Poland, and Hungary.

cases make are that the regulations 1) were unconstitutional prior restraints on speech under the First Amendment, 2) violated the plaintiffs' rights to due process under the Fifth Amendment, and 3) were not authorized by the International Emergency Economic Powers Act, which the president invoked by executive order to extend the Export Administration Regulations after the Export Administration Act expired in 1994.<sup>149</sup>

The first case is that of Philip Karn, a programmer at Qualcomm, working largely on cellular technologies. Karn's case stems from his attempts to gain a license to export source code for cryptographic algorithms printed in Bruce Schneier's *Applied Cryptography: Protocols, Algorithms and Source Code in C*. Both the Department of State and subsequently the Department of Commerce determined that the book (including source code) was in the "public domain" and freely exportable, but that the same source code in electronic format could not be exported. Karn claimed the restrictions on these algorithms helped show the irrationality of the encryption export controls because, among other things, the algorithm was developed abroad and was already available internationally as part of PGP version 5.0i.

The United States brought the case in the United States District Court for the District of Columbia. In 1996, Judge Richey granted summary judgment to the government. The court rejected Karn's claims. It held that the export restrictions did not violate the First Amendment.<sup>150</sup> On January 21, 1997, the D.C. Circuit remanded the case to the district court in light of the transfer of the export controls to the

---

<sup>148</sup> See Bureau of Export Administration Press Release, *U.S. Updates Encryption Export Rules to European Union and Other Trading Partners* (visited Dec. 14, 2000) <<http://www.bxa.doc.gov/press/2000/EncryptionRulesUpdatedOct2K.html>>.

<sup>149</sup> *Cryptography Export Litigation* (visited May 10, 2000) <<http://www.cdt.org/crypto>>.

Department of Commerce; it did not reach the constitutional issues.<sup>151</sup> In August 1997, the Department of Commerce ruled that certain programs Karn sought to export were controlled by the EAR and subject to prior licensing. In March 1998, the government moved to dismiss this law suit. On February 18, 1999, Judge Oberdorfer granted Karn's request for an evidentiary hearing.<sup>152</sup>

In another 1996 case, law professor Peter Junger filed suit to challenge the ITAR regulations, saying they restricted his ability to teach a cryptography course, as foreign students attended his classes, and he wanted to publish his class materials on a web server. He sought to post his programs and software such as PGP and RSA source code on his web site so as to use them in his course as a demonstration of how computers work. His decision to sue came after the federal Bureau of Export Administration declared that he would need a license to post encryption source code that was printed in his textbook,<sup>153</sup> and he was denied permission to "export"<sup>154</sup> the source code by posting it on the Internet.<sup>155</sup>

The Junger case initially seemed to follow the same pattern as Karn. On July 2, 1998, in *Junger v. Daley* Judge Gwin from the United States District Court for the Northern District of Ohio granted summary judgment for the government.<sup>156</sup> He decided that "exporting source code is conduct that can occasionally have communicative elements" but that this is not enough; for the licensing scheme to be

---

<sup>150</sup> Karn v. U.S. Department of State, 925 F.Supp. 1 (D.D.C. 1996).

<sup>151</sup> Remanded, No. 96-5121, 1997 U.S. App. LEXIS 2123, at \*1 (D.C. Cir. Jan 1997) (for consideration of transfer of regulatory authority to U.S. Department of Commerce).

<sup>152</sup> Order from Oberdorfer, Feb. 18, 1999.

<sup>153</sup> David Hudson, *Federal Appeals Panel Rules Encryption Source Code is Protected Speech* (last modified Apr. 5, 2000) < <http://www.freedomforum.org/news/2000/04/2000-04-05-05.asp>>.

<sup>154</sup> For encryption software, the definition of "export" also includes publication of the software on the Internet, 65 Fed. Reg. 2492, 2496 (to be codified at 15 C.F.R. § 734.2(b)(9)(ii)).

<sup>155</sup> See *Cryptography*, *supra* note 149.

an unconstitutional prior restraint on speech it must impinge on “expression, or ... conduct commonly associated with expression,” said Judge Gwin. “Even if the Export Regulations have impaired the isolated expressive acts of academics like Plaintiff Junger, exporting software is typically non-expressive.”<sup>157</sup> Junger appealed Gwin's decision to the U.S. Court of Appeals for the Sixth Circuit. After the court heard oral arguments, the BXA amended its regulations. The new regulations relaxed export controls on encryption, though many free-speech advocates say the new regulations still infringe on free-speech rights.<sup>158</sup>

Then on April 4, 2000, the case turned in Junger's favor when the Sixth Circuit found against the government.<sup>159</sup> “Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment.”<sup>160</sup>

The third case is *Bernstein v. U.S. Department of State*, a case involving a former graduate student who claimed that the government violated his right to free speech by restricting his right to post an encryption program on the net. This case, unlike the others, started off favorably for the plaintiff, with District Court Judge Marilyn Patel of the U.S. District Court for the Northern District of California ruling that source code is speech.<sup>161</sup>

Daniel Bernstein is a mathematician and cryptographer on the faculty of the University of Illinois at Chicago. He developed a specialized cryptographic algorithm, and sought to be able to “export” the source code and an academic paper

---

<sup>156</sup> *Junger v. Daley*, 8 F. Supp. 2d 708 (N.D. Ohio 1998).

<sup>157</sup> *Id.*, at 714.

<sup>158</sup> Hudson, *supra* note 153.

<sup>159</sup> *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000).

discussing the algorithm. The export regulations, so Bernstein claimed, prevented him from discussing his work at public meetings or from publishing the work. As a result, he claimed he was unable to advance his professional reputation and career by publishing and discussing his work with his professional peers and others.

However, unlike Karn, Bernstein did not request or receive approval for the export of the same materials in print and electronic form, nor did the government make separate decisions based upon the medium of the item. Therefore, in Bernstein's case the most significant argument is in his First Amendment claims – the undeniable fact that, even if not all encryption software is protected speech, Bernstein does use his software in expressive ways.<sup>162</sup>

In August 1997, Judge Patel held that encryption software does constitute protected, expressive speech and said that the encryption export controls were unconstitutional. In her ruling, Judge Patel said that computer language, like all other forms of language, is protected by the First Amendment.<sup>163</sup> In allowing the case to continue for trial, Judge Patel said, "This court can find no meaningful difference between computer languages...and German or French. All participate in a complex system of understood meanings within specific communities."<sup>164</sup> She did, however, narrow her order pending the outcome of the government's appeal to the Ninth Circuit Court of Appeals.<sup>165</sup>

---

<sup>160</sup> *Id.*

<sup>161</sup> *Bernstein v. Department of State*, 922 F. Supp. 1426 (N.D. Cal. 1996) (*Bernstein I*).

<sup>162</sup> See *Cryptography*, *supra* 149.

<sup>163</sup> *Bernstein v. Department of State*, 974 F. Supp. 1288 (N.D. Cal. 1997) (*Bernstein III*).

<sup>164</sup> *Id.*

<sup>165</sup> *Id.*

On May 6, 1999, the Ninth Circuit Court of Appeals affirmed Judge Patel's ruling that the Export Administration Regulations constituted a prior restraint on speech.<sup>166</sup> The opinion stated, "[I]nsofar as the EAR regulations on encryption software were intended to slow the spread of secure encryption methods to foreign nations, the government is intentionally retarding the progress of the flourishing science of cryptography. To the extent the government's efforts are aimed at interdicting the flow of scientific ideas (whether expressed in source code or otherwise), as distinguished from encryption products, these efforts would appear to strike deep into the heartland of the First Amendment."<sup>167</sup>

The appeals court also said:

The government defendants appeal the grant of summary judgment to the plaintiff, Professor Daniel J. Bernstein, enjoining the enforcement of certain Export Administration Regulations that limit Bernstein's ability to distribute encryption software. We find that the EAR regulations (1) operate as a prepublication licensing scheme that burdens scientific expression, (2) vest boundless discretion in government officials, and (3) lack adequate procedural safeguards. Consequently, we hold that the challenged regulations constitute a prior restraint on speech that offends the First Amendment. Although we employ a somewhat narrower rationale than did the district court, its judgment is accordingly affirmed.<sup>168</sup>

In spite of these repeated decisions in Bernstein's favor, the government filed a motion for reconsideration on June 21, 1999, which was granted on September 30. An 11-judge en banc panel of the court re-examined the case on March 21, 2000, and remanded the case back down to the three-judge panel, after the new regulations were issued.<sup>169</sup>

According to Robert O'Neil, founder of the Thomas Jefferson Center for the

---

<sup>166</sup> Bernstein, 176 F.3d. 1132 (9th Cir. 1999).

<sup>167</sup> *Id.*

<sup>168</sup> *Id.*

<sup>169</sup> Bernstein, 192 F.3d. 1308 (9th Cir. 1999).

Protection of Free Expression, it was the April 2000 *Junger* decision which was particularly important, especially in light of the constant changes in the regulations since the case was originally filed.<sup>170</sup>

“For the first time, a federal appellate court has decided that computer programming languages are entitled to the protections of the First Amendment,”<sup>171</sup> said Raymond Vasvari, legal director for the American Civil Liberties Union of Ohio, which represented Junger. Vasvari referred to the Sixth Circuit’s decision as the *first* federal appeals court opinion because the Ninth Circuit’s opinion in *Bernstein* was being re-evaluated.<sup>172</sup>

### **Concerns About CESA and 2000 Regulations**

The January 2000 regulations were the long-awaited result of constant pressure brought to bear by the industry and private citizens concerned about their privacy and First and Fourth Amendment rights. On the surface, the new regulations were leaps and bounds more progressive than previous regulation attempts. Even with these new laws, though, concerns remained about the encryption exportation process.

In the past, government officials said they must restrict the distribution of strong encryption to prevent its export to other countries – in order to prevent criminals, both foreign and domestic, from using encryption as a shield for criminal activities. They have also argued that encryption is merely a tool for scrambling electronic messages and not a means of expression, in the face of court rulings to the

---

<sup>170</sup> Hudson, *supra* note 153.

<sup>171</sup> *Id.*

<sup>172</sup> *Id.*

contrary.<sup>173</sup> Encryption experts contend that even the newest federal regulations violate their privacy and First Amendment free-expression rights to produce, use and distribute such messages.<sup>174</sup> “Now that the administration has tacitly admitted that it can’t and shouldn’t control the use of encryption, it should have announced a simple deregulation, rather than a regulatory maze,” said Barry Steinhardt, associate director for the American Civil Liberties Union.

“The bad news is that the regulations remain very complicated, and people still need to take care before sending strong encryption products abroad,” said Alan Davidson, staff counsel for the nonprofit Center for Democracy and Technology.

Organizations such as the ACLU, EFF, and EPIC in their joint statement contend the regulations are more than confusing. Specifically, they say the regulations impose special restrictions on Internet speech, a violation of the U.S. Supreme Court’s ruling in the 1997 case *Reno v. ACLU*, which said online speech enjoys a high level of protection.<sup>175</sup> They note that the same information restricted online may be legally distributed here and abroad on a piece of paper or in a book.<sup>176</sup>

### **Previous Relevant Cases**

There are non-encryption cases which argue for the general proposition that encryption should be classified as speech. In *United States v. The Progressive*, the

---

<sup>173</sup> Phillip Taylor, *Free-Speech Advocates Say Revised Encryption Regulations Fall Short* (last modified Jan. 20, 2000) <<http://www.freedomforum.org/speech/2000/1/20encryption.asp>>.

<sup>174</sup> *Id.*

<sup>175</sup> *Reno v. ACLU* 521 U.S. 844 (1997).

<sup>176</sup> *Id.*

functional aspects of technical information in the Progressive magazine article about hydrogen weapons were considered speech.<sup>177</sup>

In *Yniguez v. Arizonans for Official English*, the court said that, “Language is by definition speech, and the regulation of any language is the regulation of speech” and “...the choice to use a given language may often simply be based on a pragmatic desire to convey information to someone so that they may understand it.”<sup>178</sup>

However, even within First Amendment protections, all messages are not created equal. While the government might have a compelling interest in intercepting and decoding messages between plotting terrorists, the government would have to meet a considerably higher standard in justifying the interception of conversations between private citizens.<sup>179</sup> There are different kinds of speech that warrant different levels of protection. There is also a need to consider whether the interests are commercial or private.<sup>180</sup>

The Court has attempted to balance the First Amendment with the government’s interest in national security before. There is no need to invent a completely new standard to apply in determining how far the government can go in intercepting, decoding and regulating encryption. One idea is to use the “clear and present danger” test first developed in *Schenck*<sup>181</sup> to provide a basis for considering when the government may limit speech.<sup>182</sup> A suggested application of the test would indicate that before government can halt or punish speech, it must show 1) an

---

<sup>177</sup> *United States v. The Progressive, Inc.*, 467 F. Supp. 990, 992 (W.D. Wisc. 1979).

<sup>178</sup> *Yniguez v. Arizonans for Official English*, 42 F.3d 1217 (9th Cir. 1995).

<sup>179</sup> *Huffman et al.*, *supra* note 21.

<sup>180</sup> *Id.*

<sup>181</sup> *Schenck v. United States*, 249 U.S. 47 (1919).

<sup>182</sup> *Huffman et al.*, *supra* note 21.

objective proof of a serious danger, and 2) convincing evidence that the danger is immediate, and not remote.<sup>183</sup>

The government argues that unless it is allowed to regulate cryptography, terrorists, organized crime leaders, drug dealers, and other dangerous groups in society will use encryption as a tool to help them commit crimes and avoid detection. Similar arguments have been made in the past about books, magazines, and radio channels, all to no avail because of the presence of the First Amendment to the Constitution.<sup>184</sup> Many of these arguments are also made specious by the blatant changes in policy favoring business and commerce, and finding other ways to enhance federal agencies' means of fighting any new threats as a result of strong encryption use.

Rules on handling materials deemed sensitive to national security do not have to be changed or even challenged. The mission and goals of law enforcement agencies, including the NSA, FBI, and military also do not need changing. It is important to recognize here that the government and federal law enforcement agencies goals are not to be rejected, but need to be adapted to the current environment, and applied only in their own particular realm, and not imposed onto the day-to-day activities of those who are outside their purview. Limiting export, use, and development of encryption products and technology results in restricting expression and freedom of choice, without any corresponding guarantee of safety or security to American citizens.

---

<sup>183</sup> *Id.*

<sup>184</sup> *Id.*

## CHAPTER 6

### THE GOVERNMENT'S UNCOMPROMISING ENCRYPTION REGULATIONS

#### **Fear of Criminal Use of Encryption**

The Internet has significantly changed effectiveness of export controls. Strong encryption programs can be delivered in seconds to anywhere in the world from anywhere with a network connection. It has been increasingly difficult for countries to limit dissemination, and once a program has been released, it is nearly impossible to stop its redissemination, especially if it is a country with no export controls<sup>185</sup>

With proliferation of encryption, the U.S. government, in particular agencies like the NSA and FBI, realized that it no longer had a monopoly on the use of cryptography. Unless steps were taken to protect government ability to intercept and decode digital, encrypted communications, the government felt its own communications and national security would be placed in jeopardy. Government and law enforcement would lose some of its ability to fight crime and terrorism, and the integrity of vital communications might be subject to compromise. It was inevitable that different interests would clash, particularly as public concern about limits on free speech and the privacy of that speech continued to grow in the 1990s.<sup>186</sup>

Essentially, law enforcement advocates argue that widespread use of encryption would hamper intelligence gathering and undermine the ability of law enforcement to prevent crime. A recently published FBI report states that “encryption can also be used to conceal criminal activity and thwart law enforcement

efforts to collect critical evidence needed to prevent, solve and prosecute serious and often violent criminal activities, including illegal drug trafficking, organized crime, child pornography, and terrorism.”<sup>187</sup> For instance, law enforcement officials cite examples where strong encryption frustrated court-authorized crime interdiction efforts. Terrorist incidents also heighten fears that strong encryption has already become a vital tool used by terrorists and drug cartels to evade detection by law enforcement officials.<sup>188</sup>

Part of the stated reason for U.S. government opposition to *public* access to strong cryptography is to preserve government ability to gain access to *criminal* communications through wiretaps and computer data files seized as evidence. The usual rationale involves use of encryption by a trio of commonly agreed-upon evils – drug dealers, terrorists, and child pornographers – and the ability of law enforcement agencies to stop crimes by breaking the codes. This even though decades of wiretapping have not halted those crimes.<sup>189</sup>

Most regulation is undertaken in the name of public interest, and this is no exception. Unlike commercial broadcasting or interstate commerce where government does not participate, the government is involved in the business of cryptography through “expert” agencies such as the NSA and Sandia National Laboratories.<sup>190</sup> The government argues that unless cryptography is regulated, encryption will be used by more and more criminals and dangerous groups in society

---

<sup>185</sup> Electronic Privacy Information Center, *supra* note 109.

<sup>186</sup> Huffman et al., *supra* note 21.

<sup>187</sup> See generally FBI, Encryption: Impact on Law Enforcement (1999), at 1-17.

<sup>188</sup> Shehadeh, *supra* note 107, at 284.

<sup>189</sup> ARNOLD G. REINHOLD, CATO INSTITUTE, STRONG CRYPTOGRAPHY: THE GLOBAL TIDE OF CHANGE (1999).

<sup>190</sup> Huffman et al., *supra* note 21.

to commit crimes and avoid detection. As a result of criminal proliferation, public safety and national security will be jeopardized – and this must be avoided at all costs, even if personal freedoms are affected.<sup>191</sup>

Government interest in regulating encryption stems from its duty to ensure domestic tranquility and in maintaining law, order, and national security. Law enforcement officials argue that without the ability to decode encrypted messages, wiretapping efforts would be rendered useless.<sup>192</sup> This even though computer experts say that a \$300 million investment in computer technology could recover a 56-bit digital encryption standard (DES) key in about 12 seconds. While this is certainly expensive, it is by no means outside the ability of the government to achieve, and probably only a small fraction of the NSA budget. Few people seriously challenge government need to implement wiretaps upon a showing to a magistrate of probable cause. Nor would most people disagree that law enforcement agencies need to have tools to intercept communications of criminals seeking to commit crimes or acts of terrorism. The Constitution provides that Congress shall have the power to provide for the common defense and general welfare of the United States. Accordingly, agencies such as the NSA and FBI, as part of their defensive intelligence missions, should be able to intercept and decode encrypted messages which contain information that threatens the nation.<sup>193</sup> The problem merely remains as to what protection messages which are not criminal have from unwarranted surveillance and interception, and to what degree federal agencies really even *need* to limit encryption use.

---

<sup>191</sup> *Id.*

<sup>192</sup> *Id.*

## **Attempts to Limit Development, Exportation, and Domestic Use of Encryption**

The Clinton administration routinely invoked “national security” concerns to justify export control regulations that limit business opportunities, and in so doing cripple development of sophisticated U.S. encryption technologies. The government claims that it must have the ability to monitor communications in the digital age to protect Americans from terrorists, drug smugglers and other nefarious types. To achieve this, the Clinton administration consistently argued, the government must control the terms and conditions by which individual Americans can use sophisticated encryption technology both at home and abroad. As a comparison though, even at the height of the Cold War, the intelligence community never seriously proposed such a massive and pervasive intrusion into the lives of American citizens.<sup>194</sup>

The concerns, real or perceived, of what might happen with widespread use of encryption prompted the government to not only be concerned with exporting cryptographic products, but also with internal use. Internationally, export controls are the strongest tool used by governments to limit development and dissemination of encryption products. Export controls reduce the availability of encryption in common programs such as operating systems, electronic mail and word processors, especially from American companies.<sup>195</sup> In the United States, export controls are used to limit availability of encryption on domestic Internet sites and thus serve as indirect *domestic* controls on encryption.<sup>196</sup>

---

<sup>193</sup> *Id.*

<sup>194</sup> *Hearings on Encryption, supra* note 120.

<sup>195</sup> Electronic Privacy Information Center, *supra* note 109.

<sup>196</sup> *Id.*

The ability to encrypt and send confidential information overseas over the Internet never sat well with the U.S. government. It was concerned that this technology could be used by terrorists and terrorist countries to threaten our security.<sup>197</sup> In fact, U.S. leaders were so worried about potential use of this technology that they actually regulated the export of such encryption technology under the Arms Export Control Act. By regulating encryption technology as munitions, the U.S. government required exporters to obtain a license from the Office of Munitions Control before exporting such software. Failure to obtain a license before export could result in fines, imprisonment, or both.<sup>198</sup>

Clinton administration encryption initiatives continued after his re-election and became even more intrusive. In March 1997, the administration circulated a draft proposal for the Electronic Data Security Act of 1997, to see how legislation aimed at imposing restrictions on *domestic* encryption products might be received.<sup>199</sup>

The proposal suggested a key management infrastructure for domestic encryption use, where decryption keys would be held by “government approved” agents. While participation in the key management infrastructure would be voluntary, the administration’s proposal was criticized for making it virtually impossible to participate in electronic commerce without being part of the system.<sup>200</sup> The proposal, which Sen. Bob Kerrey (D – Neb.) sponsored, also contained provisions that would make law enforcement access to private communications easier to obtain.

---

<sup>197</sup> Grossman, *supra* note 139.

<sup>198</sup> *Id.*

<sup>199</sup> Huffman et al., *supra* note 21.

<sup>200</sup> *Id.*

While this was far from being the final word in domestic or international encryption use and export, it serves as yet another example of the many ways in which the United States government and its agencies seek to place severe limits on encryption's use – whether or not such measures are wise, or warranted.

## CHAPTER 7

### SOCIAL AND POLITICAL PROBLEMS WITH ENCRYPTION REGULATIONS

#### **Moving Beyond Old Customs**

The Clinton administration's attempts at regulating encryption were continually fraught with political and social problems. Burdensome regulations and limitations posed constitutional and privacy concerns on the part of both business and ordinary citizens. This was in large part caused by a failure of the administration to adapt its viewpoint to the changing field of encryption. Emerging computer and communications technologies radically altered the way we communicate and exchange information. Along with speed, efficiency, and cost-saving benefits of the digital revolution came new challenges to security and privacy of communication and information exchange.<sup>201</sup>

In response to these challenges, security precautions of traditional paper-based communications media – such as sealed envelopes and locked filing cabinets – are being replaced by cryptographic security techniques. By using encryption, communication and information stored and transmitted by computers can be protected against interception to an increasingly high degree.

Until the past several years, there was little non-governmental demand for encryption capability. Modern encryption technology was deployed most widely to protect the confidentiality of federal, military, and diplomatic communications. With the onset of the computer revolution and continuing innovations in encryption, a new

market for cryptographic products developed. Electronic communications are now widely used in the private and civilian sectors and are an integral component of global commerce and economy. Computers are used daily by millions of people to store and exchange an ever-increasing amount of highly personal information, including medical and financial data. In this electronic environment, the need for privacy-enhancing technologies, such as computer encryption, is clear. Communications applications such as e-mail, electronic fund transfers, and online retail require secure means of encryption – features that can only be provided if cryptographic know-how is widely available and unencumbered by government regulation.<sup>202</sup>

In 1996, the Clinton administration seemed to realize to some degree that encryption use was no longer limited to the government and military arenas, or even to terrorists and criminals. The government transferred export licensing of commercial encryption products from the State Department Munitions List to the Commerce Department's Dual-List. This classification could be used to emphasize the government's decision that strong encryption was no longer something used primarily by governments or military forces, but was an accepted part of normal commercial activity.<sup>203</sup>

### **Need for Privacy and Security for Information Transfer**

Although privacy is not specifically mentioned in the Constitution, a common law tort recognizes four distinct branches of privacy invasion, including intrusion into

---

<sup>201</sup> Electronic Privacy Information Center, *supra* note 109.

<sup>202</sup> *Id.*

<sup>203</sup> Grossman, *supra* note 139.

seclusion or solitude.<sup>204</sup> It is important for our purposes here to note that the privacy laws underwent their last major update in 1986 with enactment of the Electronic Communications Privacy Act<sup>205</sup> – which was well before e-mail, cellular phones, and the world wide web became the fixtures of business and personal lives that they are today.<sup>206</sup>

Recent and ongoing attempts to both add to law enforcement surveillance capabilities and to limit strong encryption serve to address the fact that our privacy laws have become outdated in the face of two developments: the continually growing surveillance potential of communications and computer technologies, and the federal government's expanding use of electronic monitoring and data collection techniques.<sup>207</sup> Basically, the question has become: How do we balance the need for foreign and domestic intelligence information with the responsibility to protect individual privacy rights?<sup>208</sup>

The Clinton administration made efforts to balance free speech and privacy with the needs of law enforcement and national security.<sup>209</sup> In this vein, and with more of a focus on law enforcement concerns, the administration made numerous attempts to establish national standards for encryption of voice and data communication over the rapidly growing Internet and world wide web.

---

<sup>204</sup> This categorization was suggested by Dean Prosser. William Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960). This was subsequently adopted by the Restatement of Torts (Second) at §§ 652A-652I (1977).

<sup>205</sup> 18 U.S.C. §§ 2701-2711.

<sup>206</sup> *Remarks before the Subcomm. on the Constitution of the House Judiciary Committee*, 106th Cong. (2000) (statement of James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology).

<sup>207</sup> *Id.*

<sup>208</sup> Hayden, *supra* note 68.

<sup>209</sup> Huffman et al., *supra* note 21.

Advancements in telecommunications and particularly the Internet have highlighted a fundamental, but not necessarily new privacy issue. Congress passed the Foreign Intelligence Surveillance Act<sup>210</sup> regulating the NSA's electronic surveillance in the United States.<sup>211</sup> There are times when a government needs to collect information about its citizens, but the circumstances under which this is allowed to occur either inside or outside the U.S. are extremely limited and well-regulated. Basically, there must be probable cause that a person is an agent of a foreign power and a court must issue a warrant authorizing the surveillance inside the U.S.<sup>212</sup> As detailed in Chapter 2, NSA electronic surveillance authority is found in Executive Order 12333,<sup>213</sup> which gives authorization for gathering information for intelligence and counterintelligence purposes and in support of U.S. military operations.<sup>214</sup> The agency is authorized to collect information only for *foreign* intelligence purposes<sup>215</sup> and to provide that information only to authorized government recipients. This means that NSA is not authorized to provide signals intelligence information to private U.S. companies or people.<sup>216</sup>

In all cases, intelligence collection must be conducted in a manner "consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded." These principles include not infringing on someone's right to speak, their right to speak privately if they so choose, and the Fourth Amendment prohibition against unreasonable search and seizure. Intelligence

---

<sup>210</sup> 50 U.S.C. § 1801.

<sup>211</sup> Hayden, *supra* note 68.

<sup>212</sup> *Id.*

<sup>213</sup> Exec. Order No. 12333, 3 C.F.R. 200 (1982), reprinted in 50 U.S.C. § 401 note.

<sup>214</sup> Hayden, *supra* note 68.

<sup>215</sup> The Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801(f)(2).

<sup>216</sup> Hayden, *supra* note 71.

collection must not be undertaken strictly or with the sole purpose of acquiring information concerning the domestic activities of U.S. persons.<sup>217</sup> Nevertheless, it is unavoidable that the NSA will inadvertently or coincidentally acquire information about U.S. citizens in the course of foreign intelligence collection activities.<sup>218</sup>

Separate even from NSA's eavesdropping are the efforts of the FBI and other law enforcement agencies to use new technologies to gather information on private citizens – in the name of national security. This, coupled with ever-increasing number of wiretaps, and the correspondingly increasing number of innocent conversations which are captured, emphasizes the need for people to be able to protect their communication. Though encryption regulations do not always reflect those needs, the courts are taking steps to protect privacy.

### **National Security Remains a Priority – But Not at Expense of Privacy and Free Speech**

The U.S. Federal Court of Appeals for the District of Columbia on August 15, 2000, overturned in major respects a highly contested agency ruling on wiretap standards, rejecting FBI demands for added surveillance features.<sup>219</sup> The court also signaled that interception of newer “packet” technologies must meet the highest legal standards.<sup>220</sup> In essence, the court told the FCC that it was wrong to give in to FBI surveillance demands at the cost of privacy. In a unanimous opinion, the three judge panel found that the FCC decision requiring carriers to build additional surveillance

---

<sup>217</sup> *Id.*

<sup>218</sup> Hayden, *supra* note 68.

<sup>219</sup> *US Telecom Ass'n v. FCC*, 227 F.3d 450 (D.C. Cir. 2000).

features into their networks was “an entirely unsatisfactory response” to the privacy provisions of CALEA<sup>221</sup> and failed to take into account the financial cost to industry.<sup>222</sup>

The court also concluded that government agents would be required to meet the highest legal standards if they wanted to intercept data packets that mingled addressing information and the content of communications.<sup>223</sup> It also rejected the FCC assumption that the government would be able to intercept both routing information and call content under the less demanding standard of approval required for so-called pen register and trap and trace orders.<sup>224</sup>

These attempts by the FBI to extend CALEA’s provisions to the Internet once again bring up the issue of surveillance laws’ privacy protections as they exist now.

- Data stored on networks is not afforded full privacy protection. Once something is stored on a server, it can be accessed by the government without notice to the user, and without probable cause;
- The standard for pen registers is minimal. Judges must rubber stamp any application presented to them; and
- Many protections in the wiretap law, including the special approval requirements and the statutory rule against use of illegally obtained evidence, do not apply to e-mail<sup>225</sup> and other Internet communications.<sup>226</sup>

---

<sup>220</sup> THE CENTER FOR DEMOCRACY AND TECHNOLOGY, POLICY POST VOL. 6 No.15, A BRIEFING ON PUBLIC POLICY ISSUES AFFECTING CIVIL LIBERTIES ONLINE (2000).

<sup>221</sup> The Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in sections 18 U.S.C. and 47 U.S.C.).

<sup>222</sup> *US Telecom Ass’n v. FCC*, 227 F.3d 450 (D.C. Cir. 2000).

<sup>223</sup> *Id.*

<sup>224</sup> *Id.*

<sup>225</sup> CALEA does not cover “information services” such as e-mail and Internet access. 47 U.S.C. § 1001(8)(C)(i), 1002(b)(2)(A).

There is no need to challenge continuing need for NSA, FBI, and military intelligence agencies to stay abreast of foreign intelligence – but limiting development of cryptography in the United States will not help that. We also need to recognize the continuing need to protect our own information and networks and again, limiting our development and the desire for industry to invest in such development will only hinder our national security interests in information protection, and our ability to protect online communications from “unintentional” surveillance.

### **Reasonable Expectation of Privacy Over the Internet?**

Courts may have found that consumers have no “expectation of privacy” in the digits they dial on a telephone, making pen registers and similar law enforcement listening devices dependent on a very low standard for approval. However, it may very well be that, given the revealing nature of Internet transactional information, users do have a reasonable expectation of privacy in the uniform resource locators (URLs) of web sites they visit and the email addresses of those with whom they communicate.<sup>227</sup> This is part of the reasoning behind the court’s acceptance of the need to hold up a higher standard for intercepting communication over the Internet.

The government argues that using and storing information in this manner is a choice people make – you can keep the data in your own home and you can stay off the Internet if you care about privacy. But in a world where the Internet is increasingly essential for access to commerce, community, and government services,

---

<sup>226</sup> *Internet Security and Privacy: Testimony Before the Senate Judiciary Committee*, 106th Cong. (2000) (statement of James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology).

taking advantage of online services should not come at the expense of personal privacy.<sup>228</sup> This raises the general question of whether or not there is a reasonable expectation of privacy on the Internet, and why speech and its protections should be regulated differently over the Internet than over other media.

Technological advances have repeatedly produced new forms of media, from broadcasting to cable television to the Internet. In its treatment of these new media, the Supreme Court has typically reasoned that “differences in the characteristics of new media justify differences in the First Amendment standards applied to them.”<sup>229</sup> In practice, this approach has resulted in differing levels of protection for different media – usually a lower level of protection for electronic media than for print media.<sup>230</sup> This lower level of protection comes from several concerns, but primarily the court seems to rely on ideas of the technological characteristics of the media to justify any government regulations. Although the print medium has always enjoyed the highest First Amendment protection, new electronic media have been relegated to subordinate positions and subjected to greater government regulation. In the meantime, the electronic word has become the most prevalent form of communication in our society.<sup>231</sup>

Given the trend toward electronic convergence, soon it is likely that we will see newspapers, television programs, movies, phone calls, computer data, commercial services, and many other forms of information and communication all reduced to the

---

<sup>227</sup> *Carnivore's Challenge To Privacy and Security Online: Testimony Before Subcomm. on the Constitution of the House Comm. On The Judiciary*, 106th Cong. (2000) (statement of Alan B. Davidson, Staff Counsel, Center for Democracy and Technology).

<sup>228</sup> *Id.*

<sup>229</sup> *Red Lion Broadcasting Co. v. FCC*, 395 U.S. 367, 386 (1969).

<sup>230</sup> *The Message In The Medium: The First Amendment On The Information Superhighway*, HARV. L. REV. (1994).

same format – digital bits – and all sent along the same medium – most likely fiber optic cables. Even newspapers are available online. Books and magazines are available in digital form. New music and musical groups are introduced and played over the Internet and on the computer. What once were separate fixtures in households will converge, in function if not in form. Although the ultimate synergy of these technologies may still be years away, the distinctions used to draw different free speech protections have already blurred.<sup>232</sup>

Technological characteristics can no longer be the crucial factor in determining the protection a message receives under the First Amendment. A political editorial is still a political editorial whether it is printed in a newspaper, broadcast as teletext on a television screen, downloaded from a computer network, or faxed over a phone line.<sup>233</sup> And in line with this reasoning, in *Reno v. ACLU*, the Court awarded a high level of free speech protection to Internet communications.<sup>234</sup> In its *Reno* decision, the court set forth clear guidance on the importance of free speech on the Internet.<sup>235</sup> The court made detailed findings of fact regarding the history and technology of the Internet, recognizing that it is a decentralized, global medium of communications that links people throughout the world. The court found speech over the unique medium of Internet communication deserved full First Amendment protection. (The special attributes of Internet communications were reviewed, and it was concluded that the Internet, in being “the most participatory

---

<sup>231</sup> *Id.*

<sup>232</sup> *Id.*

<sup>233</sup> *Id.*

<sup>234</sup> *Reno v. ACLU* 521 U.S. 844 (1997).

<sup>235</sup> *Id.*

form of mass speech yet developed,” was entitled to the highest level of First Amendment protection.<sup>236)</sup>

In *Reno*, the Court held that “the interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship.”<sup>237</sup> Ultimately, regulation of the information superhighway should be premised on the fundamental principle that the First Amendment protects messages, not media.<sup>238</sup> The Court also stated in *Reno* that “because the regulations define ‘export’ to include the use of Internet for a...we think it plain that the regulations potentially limit Bernstein’s freedom of speech in a variety of both domestic and foreign contexts.”<sup>239</sup> Encryption as a form of speech is still not a confidently decided-upon argument; but there can be no doubt that electronic communication over the Internet receives, and should continue to receive, all the protection the First Amendment can offer.

### **Market Dominance in Product Development**

When the world wide web and Internet use moved into the public domain, market forces and innovation quickly took over. To maintain their competitive lead in the digitally connected economy, both nationally and internationally, companies continually created encryption technologies. Such rapid innovation conflicts with the national security and intelligence community goal of controlling this technology.

---

<sup>236</sup> Kim L. Rapaport, *In the Wake of Reno v. ACLU: The Continued Struggle in Western Constitutional Democracies with Internet Censorship and Freedom of Speech Online*, AM. U. INT’L L. REV. (1998)

<sup>237</sup> *Reno v. ACLU* 521 U.S. 844 (1997).

<sup>238</sup> *The Message in the Medium*, *supra* note 230.

<sup>239</sup> *Reno v. ACLU*, 117 S. Ct. 2329, 2348-9 (1997).

Governments can no longer dictate the pace and scope of technological innovation.<sup>240</sup>

While law enforcement fights crime in cyberspace, it is the *commercial* Internet industry that is in the best position to prevent hacking crimes and protect critical infrastructures by building more secure products and networks.<sup>241</sup>

Hacking, unauthorized access to computers, denial of service attacks, and the theft, alteration, or destruction of data are all federal crimes, and appropriately so. But Internet security is not a problem primarily within the control of the federal government. Internet security is primarily a matter most effectively addressed by the private sector, which has built and improved upon this medium in such a short time with, in general, limited government interference. The tools for warning, diagnosing, preventing, and even investigating infrastructure attacks through computer networks would seem to rest in the hands of the private sector.<sup>242</sup>

In a speech before the Federal Communications Bar Association in Chicago, Federal Communications Commissioner Michael Powell said he often found that regulators are tempted to take actions and promulgate rules based on sunny or stormy pictures painted by advocates of action, without digging below the rhetoric and testing whether our intervention will really benefit the public.<sup>243</sup> According to Powell, it is established, without much question, that free markets work better than any other economic form to allocate resources, to inspire innovation, to maximize public welfare, and even to protect and empower individuals.<sup>244</sup>

---

<sup>240</sup> *Hearings on Encryption*, *supra* note 120.

<sup>241</sup> Dempsey, *supra* note 226.

<sup>242</sup> *Id.*

<sup>243</sup> Michael K. Powell, Remarks Before the Federal Communications Bar Assoc. (Jun. 15, 1999).

<sup>244</sup> *Id.*

However, so-called strong encryption is only “strong” relative to available computing power and the ability to crack the key. As computing power doubles every 18 months, no encryption scheme will remain strong for long; adding numbers to the key merely forestalls the inevitable. Encryption will be quickly rendered weak without constant innovation.<sup>245</sup> As private enterprise transitions from the Industrial Age to the Information Age, so must government. So far, government and federal programs are lagging behind in this adaptation.<sup>246</sup> For example, one major reason our national nuclear weapon labs cannot protect classified data from theft is that their computers use commercial operating systems (as do many military base networks). The reason such tools do not exist in commercial operating systems is not an absence of market demand – many industries have a need for such capabilities – but the fact that such tools require strong cryptography and therefore would subject the operating systems that contain them to export controls. Since our commercial software industry depends in large part on export revenue, firms have not been willing to place extraordinary importance or investment in developing those features as long as such complex limitations exist on their use.<sup>247</sup>

### **Outside Availability of Encryption Products**

Given the prevalence of all kinds of speech over the Internet at this point, and the already widespread use of encryption to protect everything from personal to financial data, attempts to limit encryption become increasingly ineffective. Also taking into consideration the ongoing innovation in this field, it is important to note

---

<sup>245</sup> *Hearings on Encryption*, *supra* note 120.

<sup>246</sup> Hayden, *supra* note 68.

the futility of trying to regulate this technology within any one country – even the United States. Cryptographic technology is so widespread that it is impossible to stop. If any major governments, terrorist organizations, or drug cartels are not now using strong cryptography, it is not because of lack of availability or lack of reliable suppliers.<sup>248</sup>

It is a simple matter of fact that export controls are futile because strong cryptography is already available to the general public, and to the “bad guys” as well. Why would drug dealers, for example – who now run private airlines, bribe judges, assassinate opponents, subvert armies – be deterred from obtaining and using widely available cryptographic software, whether or not it is from an American source?<sup>249</sup>

It is also naive to assume that, just because American encryption technology is not legally for sale on the international market, foreign governments, companies and criminals will not be able to encrypt their communications and intellectual property. Unlike, say, nuclear weapons, which require amounts of difficult-to-obtain materials to build, computer software design has virtually no barriers to entry.<sup>250</sup> No matter how strict the U.S. export controls have been, they can do nothing to stop a bright mathematician in Tokyo or Bombay from creating new means of encryption to fill the void left by American abdication of the market.<sup>251</sup>

United States exporters also make a strong argument that such development and export controls harm our economic interests by allowing foreign manufacturers to gain significant market share, which will have the affect of placing much of the

---

<sup>247</sup> Reinhold, *supra* note 189.

<sup>248</sup> *Id.*

<sup>249</sup> *Id.*

<sup>250</sup> *Hearings on Encryption, supra* note 120.

research and development in the hands of foreign nations. Jeffrey H. Smith, counsel for Americans for Computer Privacy remarked in hearings before the Subcommittee on International Economic Policy that if the United States loses its leadership position in the technology market, our national security agencies will have to obtain technical assistance from foreign sources, which is unacceptable.<sup>252</sup> In addition, U.S. technology industry representatives say that our policies compromise our own national security interests by forcing law enforcement to decode encryption designed and manufactured exclusively by foreign corporations.<sup>253</sup>

Finally, while there have been and certainly will be cases of law enforcement agencies successfully averting a crime or catching criminals as a result of monitoring communications, the FBI and other police agencies must adjust the existing framework for traditional wireline intercepts to the digital age. The existing paradigm simply cannot be imposed onto new media and new technologies. In order to achieve this adaptation, the government must admit one simple truth: Organized crime and drug cartels – or anyone seriously intending to violate the law – will attempt to buy the best encryption technology available. Preventing American industry from developing it simply means the illegal enterprises will buy the capability from Japan, Bombay, or Taiwan. Criminals may even pay American software writers to covertly develop code for them. Regardless of the method, criminals will obtain encryption technology.

The solution is not to “dumb down” the American economy and industry and bind the arms of developers behind their backs. Nor is it to assume that without

---

<sup>251</sup> *Id.*

<sup>252</sup> Shehadeh, *supra* note 107, at 283.

United States participation, development will come to any sort of standstill. The superiority of American products is not a given, especially in the face of years of burdensome limitations. Instead, law enforcement must become more responsive and adaptive to industry developments and more digitally aware.<sup>254</sup> The NSA and Sandia Labs should stay at the forefront so the country's national priorities can be accommodated in protecting U.S. information as well as breaking foreign codes. If U.S. law enforcement agencies truly are at the leading edge, they should have the ability to provide decryption capability for legally authorized law enforcement efforts, without sacrificing the quality of generally available products. So instead of law enforcement agencies making dire threats and fire and brimstone predictions about technology's spread, that they too should be – and in fact are – taking advantage of these new tools.

### **Federal Uses and the Law of Unintended Consequences**

Although the Justice Department frequently emphasizes ways in which digital technologies pose new challenges to law enforcement, the fact is that the digital revolution has been a boon to government surveillance and information collection as well.<sup>255</sup> So while the changing electronic landscape has made some traditional law enforcement functions more difficult, it has also provided tremendous new opportunities for data collection.<sup>256</sup> While the Justice Department frequently complains that digital technologies pose new challenges to law enforcement, it is

---

<sup>253</sup> *Id.*

<sup>254</sup> *Id.* at 293.

<sup>255</sup> *Carnivore's Challenge To Privacy and Security Online*, *supra* note 227.

<sup>256</sup> *Id.*

clear from the Justice Department's record, that the digital revolution has been a boon to government surveillance and collection of information.<sup>257</sup> American law enforcement agencies have made use of the new technologies in regimes which could be seen as harmful to American citizens in their own way, and will continue to do so. The FBI in its current budget request seeks additional funds to "data mine" public and private sources of digital information for their intelligence value. Yet the computer and communications privacy laws which would protect U.S. citizens from unwarranted intrusions were last updated in 1986.<sup>258</sup> These discrepancies again make it clear that the privacy of people's speech over the Internet – which is protected to the same extent, if not more than, any other medium, is being threatened – and the use of encryption to protect that speech is one clear way to combat that threat.

The newest regulations do lift some limitations which have been a drag on the forward momentum of encryption use in the United States. However, even the newest revamping of encryption regulations and CESA involve limits, confusing regulations, masses of paperwork, and too many exceptions to list. Another main element of CESA, as mentioned before and seen for its relevance here, is its proposed authorization of appropriations to the FBI of up to \$80 million for a Technical Support Center that would serve to respond to the increasing use of encryption for criminal purposes.<sup>259</sup> So law enforcement's hand is not as weakened as they would have the public believe.

---

<sup>257</sup> Dempsey, *supra* note 226.

<sup>258</sup> Dempsey, *supra* note 245.

<sup>259</sup> Shehadeh, *supra* note 107, at 297.

Unfortunately, the many rules limiting use of strong encryption, and preventing strong encryption from being built into software or computers, have made law-abiding citizens who desired privacy seem to be criminal.

Sir Thomas More, in *Utopia*, describes the perfect society – and the ways other societies fall short.<sup>260</sup> In one part, he describes the fate of those who have grown up with certain expectations, and are then punished for them. “Finally, when they grow up and commit the crimes that they were obviously destined to commit...you start punishing them. In other words, you create thieves, and then punish them for stealing!”<sup>261</sup> There is a direct analogy to be drawn between this description and our own situation. For years, Americans have had a tradition of expectations of privacy, and the right to keep their communications private. Now, at the natural inclination to use new technologies to preserve that privacy, they are treated as criminals. Hopefully, this is merely an unfortunate example of the Law of Unintended Consequences, and not any direct act toward restricting personal liberty. In either case, it is certainly a problem that needs a fix.

---

<sup>260</sup> THOMAS MORE, *UTOPIA* (1516).

<sup>261</sup> *Id.*, at 49.

## CHAPTER 8

### PROBLEMS WITH USING EXISTING MONITORING METHODS AS PRECEDENTS FOR INTERNET SURVEILLANCE

The initial thoughts behind the stringent regulation of encryption were in part the idea of encryption as a military or warfighting commodity. Regulations were molded around that purpose and constructed for that kind of control. The regulations were not aimed toward ensuring that communication between citizens and businesses could be monitored and scrutinized – the extension of encryption regulation to facilitating government monitoring of its own citizens was not a logical leap.

As mentioned before, it would seem to be clear that the government – however reluctantly – did at some point realize that encryption use had evolved beyond the world of a munition or dual-use good. This was shown not only by the constant change in attempts to regulate both domestic and international uses, but by moving oversight of encryption from the Department of State to the Department of Commerce on November 15, 1996. But the bulk of the government efforts were not only to preserve the integrity of law enforcement abilities, but to extend them – often in ways which do not hold up under close scrutiny.

#### **Courts and the Rapidly Changing Technology**

Considering the broad sweep of the digital revolution, both in our nation and internationally, it is apparent that the major problem now is not that technology is outpacing government ability to investigate crime, but that changes in communications and computer monitoring technology outpaced the free speech and

privacy protections in U.S. laws.<sup>262</sup> Federal Communications Commissioner Michael Powell has remarked that government-orchestrated industrial development is especially inappropriate in a market like the Internet. The Internet is driven aggressively by constant change, and the government simply is not responsive enough to manage such rapid change. Every rule or ruling issued is likely to be obsolete the day it is written.<sup>263</sup>

Attempts to limit development and use of strong encryption – or to legislate strength of cryptographic products people may use, export, discuss, or teach – would be outdated almost before the laws could be enacted. Initially, the Dual-Use Control List, on which encryption resides through the Wassenaar Arrangement, did not place a ceiling on the strength of exported encryption products. It also did not control encryption products that were generally available or in the public domain. So while United States encryption exporters were frustrated by domestic export policies that remained more restrictive than Wassenaar, foreign manufacturers were operating in less restrictive environments.

The European Union's movement away from regulating encryption exports, and recent reforms to French, British, and German encryption policies, demonstrate that current United States controls on encryption exports, which either mirror or are more restrictive than what the Wassenaar Arrangement sets forth, are outdated and do not reflect market realities.<sup>264</sup>

In December 1998, Wassenaar members revised the Dual-Use Control List, implementing a maximum bit length of 64-bits on exports of mass-market encryption

---

<sup>262</sup> Dempsey, *supra* note 226.

<sup>263</sup> Powell, *supra* note 243.

software.<sup>265</sup> But even after this modernization, it was still proposed that “to keep pace with technological advances, Wassenaar members should undertake a biannual review of the worldwide encryption standard, pursuant to which members would revise the Dual-Use Control List and increase the level of freely exportable encryption to meet the current standard.”<sup>266</sup> This in itself is futile – as the strength of encryption rises, so does the level of exportable encryption? Why not just allow the market to decide what encryption strengths are needed and let them be similarly disseminated. Constantly changing an international agreement to reflect the current status is a burdensome paper-pushing process; this is especially true when one takes into account the level of deference given to the Wassenaar rulings.

Most countries, especially those in Europe, do not rely on or defer to Wassenaar restrictions; or if they do, it is in name only. This is true even in Germany, which is known to place precedence on maintaining order and peace through restricting people’s speech (as in making speech about denial of the Holocaust illegal or restricting books which people may buy). Representatives of both the German government and business community suggest that Wassenaar was not designed to inhibit bona-fide civilian transactions, and that regulation of the Internet distribution of encryption products runs counter to Germany’s domestic policy, which is based on the free availability of encryption products.<sup>267</sup>

---

<sup>264</sup> Shehadeh, *supra* note 107, at 313.

<sup>265</sup> *Id.* at 275.

<sup>266</sup> Solveig Singleton, Encryption Policy for the 21st Century: A Future Without Government-Prescribed Key Recovery 7 (CATO Institute Policy Analysis No. 325, 1998).

## **The Electronic Communications Privacy Act of 1986**

Unfortunately, though surveillance and encryption rules have been promulgated for years, the Electronic Communications Privacy Act of 1986<sup>268</sup> was the last significant update to privacy standards of the electronic surveillance laws. As cellular telephone service became available, and as e-mail and other computer-to-computer communications were developing, Congress recognized that privacy law was woefully out of date. In response, Congress adopted the ECPA. This act made it clear that wireless voice communications were covered to the same degree as wireline voice communications.<sup>269</sup> However, since 1986, a huge array of advancements in available technology have occurred, including:

- The development of the Internet and the world wide web as mass media;
- The convergence of voice, data, video, and fax over wire, cable, and wireless systems;
- The proliferation of service providers in a decentralized, competitive communications market;
- The movement of information out of people's homes or offices and onto networks controlled by third parties; and
- The increasing power of hand-held computers and other mobile devices that access the Internet and data stored on networks.<sup>270</sup>

ECPA also set standards for access to stored email and other electronic communications and transactional records (subscriber identifying information, logs,

---

<sup>267</sup> *Id.*

<sup>268</sup> 18 U.S.C. §§ 2701-2711.

<sup>269</sup> Dempsey, *supra* note 226.

<sup>270</sup> *Id.*

toll records).<sup>271</sup> And it adopted the pen register and trap and trace statute, governing real-time interception of numbers dialed or otherwise transmitted on a telephone line.<sup>272</sup> A pen register collects the “electronic or other impulses” that identify the numbers dialed for outgoing calls and a trap and trace device collects the originating number for incoming calls.<sup>273</sup>

### **CALEA as Precedent for Internet Monitoring**

Every spring, the Administrative Office of the United States Courts publishes statistics on wiretap activity of federal, state and local police in the prior year. The 1999 Report on Wiretaps in Criminal Cases included the following statistics, among others: that the number of approved wiretaps was 1,350, while none were turned down at all; for each wiretap, the average number of conversations intercepted was 1,921; the average number of people intercepted was 195; the longest wiretap lasted 510 days (almost a year and a half); but the total incriminating conversations, of all those 2.6 million intercepted, was only 28.8 percent.<sup>274</sup> Which means that more than 70 percent of those conversations were deemed innocent.

One law enacted to assist law enforcement agencies’ efforts to maintain wireline eavesdropping capabilities was, and which has subsequently been referred to as a precedent for Internet surveillance, was the 1994 CALEA. Finding that new and emerging telecommunications technologies pose problems for law enforcement, Congress enacted CALEA “to preserve the government’s ability, pursuant to court

---

<sup>271</sup> *Id.* referencing 18 U.S.C. § 2701.

<sup>272</sup> *Id.*, referencing 18 U.S.C. § 3121.

<sup>273</sup> Dempsey, *supra* note 145.

<sup>274</sup> *Nature and Scope of Government Electronic Surveillance Activity* (last modified Sep. 25, 2000) <[http://www.cdt.org/digi\\_tele/wiretap\\_overview.html](http://www.cdt.org/digi_tele/wiretap_overview.html)>.

order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling, while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services.” CALEA requires telecommunications carriers and equipment manufacturers to build into their networks technical capabilities to assist law enforcement with authorized interception of communications and call-identifying information.<sup>275</sup> Because Congress intended CALEA to preserve the status quo, the act does not alter the existing legal framework for obtaining wiretap and pen register authorization, “provid[ing] law enforcement no more and no less access to information than it had in the past.”<sup>276</sup>

From a First Amendment perspective, CALEA was not a serious threat to free speech. The law maintained the status quo by upgrading technical capabilities of government agencies, who had presumably been obtaining warrants for their wiretaps. But this was only because the implications of encryption as speech had yet to be considered. Wiretapping, though intrusive, affected few people, and never included access to more information than pre-CALEA.<sup>277</sup> However, the act does not specifically cover “information services” such as e-mail or Internet access.<sup>278</sup> So when the FBI tried to increase the scope of CALEA to include packet-switched information passed over wireless phones and the Internet, the differences began to show, and threats to free speech and privacy became apparent.

---

<sup>275</sup> US Telecom Ass’n v. FCC, 227 F.3d 450 (D.C. Cir. 2000).

<sup>276</sup> *Id.*, referencing H.R. Rep. No. 103-827, pt. 1, at 22

<sup>277</sup> Huffman et al., *supra* note 21.

<sup>278</sup> 47 U.S.C. § 1001(8)(C)(i), 1002(b)(2)(A).

The D.C. Circuit on August 15, 2000, overturned in part an FCC ruling on wiretap standards under the 1994 CALEA statute.<sup>279</sup> The court rejected the FCC's decision ordering carriers to provide added call dialing and signaling information sought by the FBI as an entirely unsatisfactory response to CALEA's privacy provisions. The court based its decision on the view that the government needs a full, probable cause-based Title III wiretap order to obtain packets from which content has not been stripped, thus casting doubt on the legality of the FBI's Carnivore sniffing program when used under the weaker pen register or trap and trace standard (which does not allow for capture of content).<sup>280</sup>

### **Attempts to Transfer Pen Register and Wiretapping to Internet**

Government use of existing plain old telephone service (POTS) wiretapping and surveillance technology is intruding to an increasing degree on our rights to speak freely and privately, as shown by the 1999 statistics. In 1979, the Supreme Court held that there is no constitutionally-protected privacy interest in the numbers one dials to initiate a telephone call, data collected under a device known as a pen register.<sup>281</sup> Now the scene changes when law enforcement agencies attempt to transfer such monitoring programs as pen registers to application to wireless communication. The demand that every current offline capability be directly implemented online should not become an excuse for creating a massive technical architecture for surveillance that, given the nature of the Internet, could be far more invasive than anything we

---

<sup>279</sup> US Telecom Ass'n v. FCC, 227 F.3d 450 (D.C. Cir. 2000).

<sup>280</sup> *Id.*

<sup>281</sup> Dempsey, *supra* note 145.

have seen to date.<sup>282</sup> Protecting national security and public safety in the digital age is a major challenge and priority for our country. At the same time, the desire to fix the online world should not be carried out unchecked, disregarding the huge privacy and security risks.<sup>283</sup>

With the evolution of technology and communication, personal data is moving out of the desk drawer and onto the Internet. Does this mean that information is being stored more and more in configurations not protected by the Fourth Amendment? The government argues that this is a choice people make -people can keep the data on their own server and stay off the Internet if they care about privacy. But this is a little like arguing that you lose your privacy rights when you choose to communicate using the services of a telephone company, and if you want to preserve your privacy you should visit the person and have a face-to-face conversation.<sup>284</sup>

The Supreme Court has ruled that there is an expectation of privacy in communications, but has also taken steps that had serious adverse consequences for privacy: It held that personal information given to a third party loses its Fourth Amendment protection.<sup>285</sup> This rule now serves as the basis for government access to all records that constitute a profile of our lives, both online and offline: credit, medical, purchasing, travel, car rental, etc. In the absence of a specific statute, these records are available to law enforcement for the asking and can be compelled by subpoena issued without meaningful judicial control. The implications of this “third party record” rule are seen in the Clinton administration’s proposed Cyberspace

---

<sup>282</sup> *Carnivore’s Challenge To Privacy and Security Online*, *supra* note 227.

<sup>283</sup> *Id.*

<sup>284</sup> Dempsey, *supra* note 145.

<sup>285</sup> *United States v. Miller*, 425 U.S. 435 (1976).

Electronic Security Act, discussed earlier, which would allow the government to obtain encryption keys or other decryption information from third parties under a court order procedure that would provide neither probable cause nor notice protections of the Fourth Amendment.<sup>286</sup>

Currently, if the government wants access to actual, physical papers or effects in your home or office, it has to meet a high standard: the government must obtain a warrant from a judge based on a showing of probable cause to believe that a crime has been, is being or is about to be committed and that the search will uncover evidence of the crime. The warrant must particularly describe the place to be searched and the things to be seized; and the government must provide you with contemporaneous notice of the search and an inventory of items taken. These rules continue to apply in the computer age – but only so long as you keep information stored on your hard drive or disks in your home or office.<sup>287</sup>

But now, the government wants to extend the pen register statute to the Internet and create a roving pen register authority – one not fixed to a particular time and place. Yet the low standard for pen registers imposes no effective control on the government, reducing judges to mere rubber-stamps. Pen register authority as applied to Internet communications is even more revealing.<sup>288</sup> The transactional or addressing data for electronic communications like email and web browsing can be much more revealing than telephone numbers dialed. First, e-mail addresses are more personally revealing than phone numbers because email addresses are unique to individual users. Furthermore, if the pen register authority were to apply to URLs or

---

<sup>286</sup> Dempsey, *supra* note 145.

<sup>287</sup> *Id.*

the names of files transmitted under a file transfer protocol, then the addressing information would actually convey the substance of a communication – information normally excluded under pen register collection.<sup>289</sup>

One such attempt at using the Internet to monitor citizens' speech is the FBI's computer program Carnivore. The FBI's apparent attempt to extend pen registers and trap and trace orders for telephone surveillance into the Internet is not a simple matter. Capturing Internet origin and destination addresses instead of numbers dialed could create a much more intrusive form of surveillance not clearly supported by law, and not justified given the current low standard for authorization.<sup>290</sup> Finding the addressee of an email or the name of a web site being visited - if that is what law enforcement is seeking - will often require analysis of the content of packets, not just the header information.<sup>291</sup> The Carnivore concept demands greater public oversight and attention. More broadly, it speaks to the need for modernization of surveillance laws and greater privacy protections to counteract the real threats to privacy online.<sup>292</sup> Carnivore shows how traditional conceptions of wiretapping and the Fourth Amendment, developed in an era of central-switch telephone networks, do not neatly translate onto the packetized, decentralized Internet.<sup>293</sup>

---

<sup>288</sup> Dempsey, *supra* note 226.

<sup>289</sup> Dempsey, *supra* note 145.

<sup>290</sup> *Carnivore's Challenge To Privacy and Security Online*, *supra* note 227.

<sup>291</sup> *Id.*

<sup>292</sup> *Id.*

<sup>293</sup> *Id.*

## **Fourth Amendment Conflicts With Electronic Surveillance, and Encryption Limitations**

Supreme Court cases establish limits on how far the government can go in searching and seizing. The Fourth Amendment, which protects people and their property from unreasonable searches and seizures, has been the topic of a number of such defenses. For example, in *Berger v. New York*, the Supreme Court reversed a bribery conviction on the grounds that a New York statute authorizing the recording of a conversation violated the Fourth and Fourteenth Amendments to the Constitution. Eavesdropping was permissible, the Court said, but only when properly conducted and appropriately authorized by the court.<sup>294</sup> Also, in *Katz v. United States*, the Court said physical intrusion did not have to take place in order for an unwarranted intrusion to occur. The “Fourth Amendment protects people, not places.”<sup>295</sup>

In *Berger v. New York*, the Supreme Court held unconstitutional on its face a state eavesdropping statute under which judges were authorized to issue warrants permitting police officers to trespass on private premises to install listening devices.<sup>296</sup> The warrants were to be issued upon a showing of “reasonable ground to believe that evidence of crime may be thus obtained, and particularly describing the person or persons whose communications, conversations or discussions are to be overheard or recorded.” For the five-justice majority, Justice Clark discerned several constitutional defects in the law.<sup>297</sup>

---

<sup>294</sup> *Berger v. New York*, 388 U.S. 41 (1967).

<sup>295</sup> *Katz v. United States*, 389 U.S. 347, at 353.

<sup>296</sup> *Berger v. New York*, 388 U.S. 41 (1967), at 50-53.

<sup>297</sup> *Id.*

The purpose of the probable-cause requirement of the Fourth Amendment to keep the state out of constitutionally protected areas until it has reason to believe that a specific crime has been or is being committed is thereby wholly aborted.<sup>298</sup> Secondly, authorization of eavesdropping for a two-month period is the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause. During such extended surveillance, “prompt execution” is also avoided. During such a long and continuous (24 hours a day) period the conversations of any and all persons coming into the area covered by the device will be seized indiscriminately and without regard to their connection with the crime under investigation.<sup>299</sup> In light of this, the very long eavesdropping operations reflected in the 1999 statistics seem unbelievably excessive.

Two bills, the Electronic Communications Privacy Act of 2000 and the Digital Privacy Act of 2000 (H.R.s 5018 and 4987), address Fourth Amendment privacy issues - the rules for government monitoring of electronic communications. They would also make important improvements in the enforcement of the Constitutional guarantee against unreasonable searches and seizures.<sup>300</sup>

There has been a steady increase in the number of wiretaps yearly, in the average length of wiretaps, in the number of conversations intercepted per tap, and in the number of persons whose conversations are intercepted per tap. Interestingly, they

---

<sup>298</sup> *Electronic Surveillance and the Fourth Amendment* (visited Dec. 29, 2000) <<http://caselaw.lp.findlaw.com/data/constitution/amendment04/f132>>.

<sup>299</sup> *Id.*

<sup>300</sup> Dempsey, *supra* note 226.

have shown a significant decrease in the percentage of incriminating conversations per tap.<sup>301</sup>

Part of the Digital Privacy Act would amend the pen register and trap and trace statute from its almost non-existent standard to require a finding that the factual evidence underpinning the government's application for a surveillance order "reasonably indicates that a crime has been, is being, or will be committed, and information likely to be obtained by such installation and use [of the pen register or trap and trace device] is relevant to the investigation of that crime." The reasonable indication standard is a low standard, but at the same time is a very practical and well tested standard. In fact, the reasonable indication standard is the standard used in the Justice Department's guidelines for criminal and terrorist investigations.<sup>302</sup>

Unanimously, the Court held that at least in cases of domestic subversive investigations, compliance with the warrant provisions of the Fourth Amendment was required.<sup>303</sup> That is, it held up the point that the "government's duty to preserve the national security did *not* override the guarantee that before government could invade the privacy of its citizens it must present to a neutral magistrate evidence sufficient to support issuance of a warrant authorizing that invasion of privacy."<sup>304</sup>

We do not need a new Fourth Amendment for cyberspace, any more than we need a new First Amendment for every new medium and new technology. The one we have is good enough. But we need to recognize that people are conducting more and more of their lives online. It should not be the end of the privacy debate to say

---

<sup>301</sup> *Id.*

<sup>302</sup> *Id.*

<sup>303</sup> *Electronic Surveillance and the Fourth Amendment*, *supra* note 298.

<sup>304</sup> *Id.* [emphasis added]

that technological change takes information outside the protection of the Fourth Amendment as interpreted by the courts 25 years ago. Nor is it adequate to say that individuals are voluntarily surrendering their privacy by using new computer and communications technologies. What we need is to translate the Fourth Amendment's vision of limited government power and personal privacy to the global, decentralized, networked environment of the Internet.<sup>305</sup> Every achievement in the name of free speech and privacy is significant, inasmuch as the tendency of government so often is to regard opponents of its policies as a threat and hence to tread in areas protected by the First Amendment as well as by the Fourth.<sup>306</sup>

---

<sup>305</sup> Dempsey, *supra* note 145.

<sup>306</sup> *Electronic Surveillance and the Fourth Amendment*, *supra* note 298.

## CHAPTER 9

### CONCLUSIONS AND RECOMMENDATIONS

*“Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.”*

- Article 19, International Covenant on Civil and Political Rights

New uses and the changing environment of the Internet calls for new perspectives for regulation. It is necessary to keep in mind the constitutional protections in place to protect our freedom to speak when and how we choose, and nothing about keeping that freedom private should change those protections. Though privacy protections per se are not found in the constitution, there is an established common law and statutory precedent of personal privacy, even while communication over “public” utilities, such as the telephone, and media. Internet communication has been granted a great deal of First Amendment protection as a new and democratic means of communication.<sup>307</sup> While it is true that criminals may make ill use of the privilege of strong encryption technology, that alone should not prevent the privilege from existing.

Considering the broad sweep of the digital revolution, both in our nation and internationally, it is apparent that a major problem is that changing communications technology is outpacing the free speech and privacy protections in our laws.<sup>308</sup> The Internet is driven aggressively by constant change, and the government simply is not responsive enough to manage such rapid change. Every rule or ruling issued is likely

---

<sup>307</sup> Reno v. ACLU 521 U.S. 844 (1997).

to be obsolete the day it is written.<sup>309</sup> What is seen throughout the Clinton administration is a desperate attempt by government and its law enforcement agencies to maintain control over an increasingly unregulated technology, used with a new, basically unregulated medium. The Clinton administration saw one possible outcome – of not being able to adapt quickly enough – and instead of advancing the government’s own ability, sought to limit the rights of everyone else.

Originally only available and used by military agencies, strong encryption is now available to many and has become a building block for the new digital economy. It is essential to provide security and privacy for electronic commerce and e-business. Encryption is critical because it allows individuals, businesses, and other organizations to share information privately without its being unlawfully intercepted or accessed by a third party, to establish their identities, and to maintain the integrity of information.<sup>310</sup>

America’s interests do not end at the borders. American diplomats, servicemembers, as well as countless business people work and live around the globe. National interests are served by the ability to securely send and receive proprietary, personal, and classified information to exactly where it is needed all over the world.<sup>311</sup> Twenty years ago the Defense Department operated largely proprietary communications systems over government-owned switches and circuits. Department of Defense technology was “homebuilt” and tightly controlled. Today, the DoD has more computer users than any other organization in the world – 2.1 million

---

<sup>308</sup> Dempsey, *supra* note 226.

<sup>309</sup> Powell, *supra* note 243.

<sup>310</sup> Cohen et al., *supra* note 41.

<sup>311</sup> *Id.*

computers access more than 10,000 networks on an average work day.<sup>312</sup> Even so, 95 percent of DoD's communications occur over public circuits or with commercial software and hardware. The Defense Department's reliance on commercial products and services is repeated throughout the country by government agencies and the private sector.<sup>313</sup> This emphasizes all the more the necessity for not restricting industry's strong encryption development and use. The National Research Council's Committee to Study National Cryptography Policy pointed out as early as 1996 that:

If cryptography can protect the trade secrets and proprietary information of businesses and thereby reduce economic espionage (which it can), it also supports in a most important manner the job of law enforcement. If cryptography can help protect nationally critical information systems and networks against unauthorized penetration (which it can), it also supports the national security of the United States.<sup>314</sup>

The government has ostensibly tried to maintain a balance between privacy and commercial interests on one hand and public safety and national security concerns on the other – by limiting the export of strong encryption software. This has become increasingly difficult with the growing need for strong encryption for electronic commerce, growing sophistication of foreign encryption products and the abundance of vendors. No one has been satisfied with the resulting attempts at legislation. American companies and individuals demand that strong encryption be integrated into computer systems, networks, and applications. National security organizations worry that the uncontrolled export of encryption will result in diversion of powerful tools to questionable end users (terrorists, etc.). Law enforcement

---

<sup>312</sup> *Id.*

<sup>313</sup> *Id.*

organizations see criminals increasingly adopting tools that put them beyond the reach of lawful surveillance.<sup>315</sup> There are fears of international narcotics traffickers routinely using computer messages to communicate with each other, cyber-warfare efforts by hostile governments, and pedophiles stalking children in computer chat rooms.<sup>316</sup>

National Security Agency and military schemes for control over information are very rigorous. Members of these organizations are subject to strict control and monitoring, and follow specific protocols for the transfer and handling of information. These security measures have to do with the importance of maintaining control over information, especially classified information, in the interests of national security. While security is also important in the public sector, members of the public have never been subject to military regulations – as not only would that be inappropriate, but it would also drastically conflict with First Amendment rights.

Rules on the handling of materials deemed sensitive to national security do not have to be changed or even challenged. The mission and goals of law enforcement agencies, including the NSA, FBI, and military also do not need changing. The stiff DoD regulations should continue to be applied – but only in their own particular realm, and not juxtaposed onto the day-to-day activities of those who are outside their purview. Limiting industry export and use and development of encryption technology results in restricting expression and freedom of choice, without any corresponding guarantee of safety or security to American citizens.

---

<sup>314</sup> National Research Council Report. See also, G.A. Keyworth, II and David E. Colton, *The Progress and Freedom Foundation, The Computer Revolution, Encryption And True Threats to National Security* (June 1996).

<sup>315</sup> Cohen et al., *supra* note 285.

This is true now more than ever, since it has been established in recent court cases that speech over the Internet earns the highest degree of First Amendment protection available, and that even computer code and encryption codes are a form of speech (and entitled to First Amendment protections). We have established a right to speak freely and privately over the Internet – and restrictive encryption legislation conflicts with that privacy. It is true that federal law enforcement agencies are responsible to society and the people, but this is not an adequate justification for suppressing the U.S. market in a new technology in response to the fear that they may not always be up to meeting each new challenge. The purpose of law enforcement and the military are to protect our country from injustices, and protect our liberties. When the government takes action that unnecessarily curtails our liberties and freedoms, it makes a mockery of the basic principles upon which our nation was founded.

Free citizens must have the ability to conduct direct, instantaneous, spontaneous, and private communication using whatever technology is available. Without the knowledge and assurance that private communications are, indeed, private, habits based upon fear and insecurity will gradually replace habits of freedom.<sup>317</sup>

Those who have argued for mandatory back-door access and key escrow have failed to show any proof, scientific or otherwise, that “bad guys” are incapable of seeking out strong encryption without key escrow features. Criminals are likely to use the strongest encryption for their communication. Those involved in planning

---

<sup>316</sup> *Id.*

capital crimes will not be worried about violating cryptography laws.<sup>318</sup> These decisions are not dependent on the availability of American products. No geographic attribute significantly influences the qualities necessary to be a cryptographer or gives citizens of one nation any advantage over those of another.<sup>319</sup>

Even the National Security Agency admits that key recovery schemes would not solve law enforcement's problems with encrypted information. An NSA report on key recovery issued in February 1998 lists at least 18 examples of how such a system could be overcome.<sup>320</sup> The agency most consistently insisting on key escrow has been the FBI, which has also been trying to use new Internet technologies combined with old laws to justify expanding their domestic surveillance capabilities. The result was for too long export control laws that demanded an intolerable sacrifice of freedom and privacy for an ineffectual commitment to security. Encryption software and hardware simply enable one to speak in a language unknown to the government – hardly by definition an illegal or subversive act.<sup>321</sup>

We do not need a new Fourth Amendment for cyberspace, any more than we need a new First Amendment for every new medium and new technology. The one we have is good enough. But it is important to recognize people are conducting more of their lives online. It should not be the end of the privacy debate to say that technological change takes information outside the protection of the Fourth Amendment as interpreted by the courts 25 years ago. Nor is it adequate to say that

---

<sup>317</sup> AMERICAN CIVIL LIBERTIES UNION, *BIG BROTHER IN THE WIRES: WIRETAPPING IN THE DIGITAL AGE* (1998).

<sup>318</sup> HENRY B. WOLFE, , *THE MYTH OF SUPERIORITY OF AMERICAN ENCRYPTION PRODUCTS* (CATO INSTITUTE, BRIEFING PAPER No. 42, 1998).

<sup>319</sup> *Id.*

<sup>320</sup> NATIONAL SECURITY AGENCY, *THREAT AND VULNERABILITY MODEL FOR KEY RECOVERY* (1998).

individuals are voluntarily surrendering their privacy by using new computer and communications technologies. By definition, electronic surveillance constitutes a general search, not a search limited to specific objects, people and places as required by the Fourth Amendment.<sup>322</sup> What we need is to translate the Fourth Amendment's vision of limited government power and personal privacy to the global, decentralized, networked environment of the Internet.<sup>323</sup> Every achievement in the name of free speech and privacy is significant, as the tendency of government is often to regard opponents to its policies as a threat and to tread in areas protected by the First and Fourth Amendments.<sup>324</sup>

### **Bottom Line**

There is a certain sympathy to be found toward the case made by those who believe curbing criminal behavior is a worthy enough cause to justify the associated limitations to people's rights. Many make the argument that it is the government's job to take every necessary step within its power to protect the people it serves, even if this results in some restrictions on the people themselves. This argument is used in gun control – that some regulation and limitations are necessary for the greater good. In fact, a very similar argument has been made by the government in the past, regulating encryption as a dual-use munition. However, the American government opened the door to challenge that policy when it transferred the jurisdiction away

---

<sup>321</sup> Wolfe, *supra* note 318.

<sup>322</sup> American Civil Liberties Union, *supra* note 317.

<sup>323</sup> Dempsey, *supra* note 226.

<sup>324</sup> *Electronic Surveillance and the Fourth Amendment*, *supra* note 298.

from the Department of State, and designated encryption as a commodity to be regulated by the Department of Commerce.

While there is a strong case to be made in law enforcement agencies' favor for the mandatory use of key escrow, or the mandatory addition of back-doors into encryption software, analysis of the research still seems to point to these as overly intrusive fixes to the problem. The resulting infringements on American citizens' rights are an unacceptable price to pay for a system which cannot guarantee any measure of success. Criminals will continue to be able to purchase products from outside the United States without such built-in access provisions. As always, the criminal element will not feel bound by U.S. laws, and so it is the American public, using encryption products to safeguard their own information, who will suffer from the burdensome regulation.

Through much analysis, it is clear that trying to police and monitor as vast and global a network as the Internet would be both a massive and unrealistic undertaking. Whatever monitoring methodology was to be developed to track illegal use and export of strong encryption products could instead be used strictly to track the exportation and unauthorized uses of the classified DOD- and NSA-developed encryption products used in defense of the nation. This would not only protect an important aspect of national security, but would also serve to narrow the field of monitoring, since not every product above a certain strength would be subject to control.

If law enforcement agencies rely too heavily on the guarantee of industry-orchestrated access, there is the risk that those agencies will not focus enough

attention on developing their own capabilities to respond to new technology, and the successively more sophisticated products which will inevitably emerge. In light of the failure of the Wassenaar Arrangement to establish any consistent international policy, and taking into account the consistently more lenient bent of other countries toward encryption export policies, it also appears unlikely that any single policy could be found to accommodate the international community. Also, any such policy would almost certainly exclude the so-called terrorist nations, which will continue to use, create, and export encryption products to any willing to pay for the service.

The bottom line is that given the lack of any evidence that restricting strong encryption will prevent criminals from using and developing encryption products, the Clinton Administration regulations are overly burdensome. While there should be some regulation, it should remain focused on tracking only that use and export of encryption products which specifically imitate our classified DOD and NSA encryption schemes – and thus make the federal government the ideal candidate for policing for such violations. This would not affect the business or individual uses of encryption products, and would limit the ability of government to intrude onto American citizens' First and Fourth Amendment and privacy rights. The world is changing, and the American government needs to change with it, and understand that more control is not always the answer.

### **Limitations of This Study**

The move of encryption out of the national security realm and into the public domain has occurred only relatively recently in our history, becoming a serious issue

only in the last decade. While there is much literature from all points of view on the subject, most of it is opinion, and little based on hard fact. The Internet, and regulation of it, is constantly evolving as the nation and the world try to come to grips with the impact of this new medium. Changes in the world of encryption product use, dissemination, and availability have occurred steadily over the past few years, with significant changes occurring just during the evolution of this thesis. As the environment has changed, so have the regulations attempting to control the proliferation of this technology.

An examination of the constitutional conflicts with the changing regime of encryption export and use regulations, primarily seen during the Clinton administration, shows very few court cases to interpret. Only three main cases, all filed within the last four years, and not all settled yet, address the affects of the regulations on speech. The constant fighting by the U.S. government of the First Amendment virtues of encrypted electronic communication has prevented at least two of these cases from arriving at a definite conclusion. The cutoff for research was December 31, 2000.

Also, this paper does not address Fifth Amendment self-incrimination issues (as related to being forced to supply decryption keys). Nor does it go into intellectual property rights, or rights of businesses to maintain security of their proprietary information.

Finally, there are certain limitations pertaining to the lack of available material from DoD and other defense agencies, either because such information is classified, or is in other ways barred from public viewing. Many of the Air Force and DoD

manuals and regulations detailing how information is classified, and some of the particular ways such information is handled, are considered For Official Use Only (FOUO), or marked at varying levels of secret classification.

### **Suggestions for Further Research**

There are many ways to expand on this topic. Not the least of these avenues would focus on comparing the final outcome and comparison of the two ongoing cases challenging the constitutionality of the encryption regulations (*Junger* and *Bernstein*).

It would also be interesting to study the further development of encryption technology and use in the public sphere, after the current policy has been in effect in the United States for a few years. This would include examining the results of the more relaxed export regulations, and allocation of more monies and resources to agencies such as the FBI to combat the challenge of criminal uses of encryption. What will the track record be of intercepting and using encrypted files to prosecute criminals? Also, with the government's apparent acceptance of strong encryption use, will more enhanced surveillance capabilities continue to be pursued (such as requested under CALEA or attempted with Carnivore)?

Along with changes in U.S. policy and technology development, it would be worth looking at what effect the newest regulations have on existing international agreements, such as the Wassenaar Arrangement.

One final suggestion would be to undertake a thorough examination of what the consequences would be of removing export regulations almost entirely, except as

related to the seven designated terrorist nations and for established cases of espionage or other criminal offense.

## BIBLIOGRAPHY

### **Case Citations**

Bernstein v. United States Department of State, 922 F. Supp. 1426 (N.D. Cal. 1996).  
[Bernstein I]

Bernstein v. United States, 1999 U.S. App. LEXIS 8595 (9th Cir. 1999). [Bernstein  
III]

Karn v. U.S. Department of State, 925 F.Supp. 1 (D.D.C. 1996).

Junger v. Daley N.D. Ohio, 1:96-CV-1723.

Red Lion Broadcasting Co. v. FCC, 395 U.S. 367, 386 (1969).

Reno v. ACLU 117 S.Ct. 2329 (1997).

Schenck v. United States, 249 U.S. 47, 30 S. CT. 247, 63 L. ED. 470 (1919).

United States v. Miller, 425 U.S. 435 (1976).

U.S. Telecom Ass'n v. FCC (2000).

### **U.S. Statutes and Regulations**

Arms Export Control Act, 22 U.S.C. §§ 2751-2799aa-2.

The Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108  
Stat. 4279 (1994) (codified as amended in sections 18 U.S.C. and 47 U.S.C.).

The Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2701-2711.

Exec. Order No. 12333, 3 C.F.R. 200 (1982), reprinted in 50 U.S.C. § 401 note.

Export Administration Regulations, 15 C.F.R. Parts 730-774.

The Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 et seq.

International Traffic in Arms Regulations, 22 C.F.R. (1995).

Promote Reliable On-Line Transactions to Encourage Commerce and Trade Act, S.  
798, 106th Cong. (1999).

The Security and Freedom Through Encryption Act, H.R. 850, 106th Cong. (1999).

U.S. Munitions List, 22 C.F.R. §§ 121.1-.15.

### **Government Instructions**

Air Force Instruction 33-210 Cryptographic Access Program (19 May 2000).

Air Force Instruction 33-210 Cryptographic Access Program(19 May 2000)

Air Force Instruction 31-401 Information Security Program Management(1 Jan 1999)

Air Force Instruction 33-216 Management of Manual Cryptosystems(1 Nov 1997)

Air Force Policy Directive 31-4 Information Security (1 Sep 1998)

Air Force Policy Directive 61-2 Management Of Scientific and Technical Information (7 Apr 1993)

Air Force Policy Directive 71-1 Criminal Investigations and Counterintelligence(1 Jul 1999)

Department of Defense 5200.1-H Department of Defense Handbook for Writing Security Classification Guidance (Nov 99)

Department of Defense 5200.1-R Information Security Program (Jan 1997)

Department of Defense 5220.22-S COMSEC Supplement to Industrial Security Manual for Safeguarding Classified Information (Mar 1988)

### **Hearings**

*Carnivore's Challenge To Privacy and Security Online: Testimony Before Subcomm. on the Constitution of the House Comm. On The Judiciary*, 106th Cong. (2000) (statement of Alan B. Davidson, Staff Counsel, Center for Democracy and Technology).

*Carnivore Diagnostic Tool, Statement for the Record Before the United States Senate The Committee on the Judiciary*, 106th Cong. (2000) (statement of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation).

*The Fourth Amendment and the Internet, Testimony Before the Subcomm. on the Constitution of the House Judiciary Comm.*, 106th Cong. (2000) (statement by James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology).

*Hearings on Encryption Before the Subcommittee on Telecommunications, Trade And Consumer Protection of the Committee On Commerce*, 105th Cong. (1997) (statement of George A. Keyworth, II).

*Internet Security and Privacy: Testimony Before the Senate Judiciary Committee*, 106th Cong. (2000) (statement of James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology).

*Remarks before the Subcomm. on the Constitution of the House Judiciary Committee*, 106th Cong. (2000) (statement of James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology).

*Testimony Before the House Permanent Select Committee on Intelligence*, 106th Cong. (2000) (statement of Lt. Gen. Michael V. Hayden, USAF, Director, National Security Agency).

### **Speeches**

Lt. Gen. Michael V. Hayden, Address at the Kennedy Political Union of American University (Feb. 17, 2000).

Michael K. Powell, Remarks Before the Federal Communications Bar Assoc. (Jun. 15, 1999).

Solveig Singleton, Privacy Issues In Federal Systems: A Constitutional Perspective, Remarks before the National Institute of Standards and Technology Computer System Security and Privacy Advisory Board Meeting (Mar. 17, 1999).

### **Books, Periodicals**

Mark Grossman, *Unscrambling the Rules on Encryption*, BROWARD DAILY BUS. REV., Apr. 18, 2000, at A1.

John L. Huffman et al., *Encryption and the First Amendment*, 2 COMM. L. & POLICY (1997).

David Loundy, *Try Decoding The Latest In Munitions-Wear*, CHI. DAILY L. BULL., Sept. 14, 1995, at 6.

David Loundy, *Congress Scrambles To Address Encryption Issues*, CHI. DAILY L. BULL., Mar. 13, 1997, at 5.

*The Message In The Medium: The First Amendment On The Information Superhighway*, HARV. L. REV. (1994).

Aaron Pressman, *Senators Call For Mandatory US Encryption Controls*, Sep. 4, 1997.

Kim L. Rapaport, In the Wake of Reno v. ACLU: The Continued Struggle in Western Constitutional Democracies with Internet Censorship and Freedom of Speech Online, AM. U. INT'L L. REV. (1998).

Karim K. Shehadeh, *The Wassenaar Arrangement and Encryption Exports: An Ineffective Export Control Regime that Compromises United States' Economic Interests*, 15 AM. U. INT'L L. REV. 271 (1999).

SIMON SINGH, *THE CODE BOOK* (1999).

*Monday E-Privacy Act Attempts Encryption Compromise*, N.Y. L.J., May 18, 1998, at S11.

### **Online Resources**

Amy Branson and Dan Froomkin, *Deciphering Encryption* (last modified May 8, 1998) <[www.washingtonpost.com/wp-srv/politics/special/encryption/keystories.htm](http://www.washingtonpost.com/wp-srv/politics/special/encryption/keystories.htm)>.

Bert-Jaap Koops, *Crypto Law Survey: Version 17.0, February 2000* (visited May 4, 2000) <<http://cwis.kub.nl/~frw/people/koops/lawsurvey.htm>>.

*A Brief History of the Internet and Related Networks* (visited Feb. 25, 2000) <<http://www.isoc.org/internet/history/cerf.html>>.

Bureau of Export Administration Press Release, *U.S. Updates Encryption Export Rules to European Union and Other Trading Partners* (visited Dec. 14, 2000) <<http://www.bxa.doc.gov/press/2000/EncryptionRulesUpdatedOct2K.html>>.

William Cohen et al., *Preserving America's Privacy And Security In The Next Century: A Strategy For America In Cyberspace: A Report To The President Of The United States* (last modified Sep. 16, 1999) <[www.Cdt.Org/Crypto/CESA/Cesawhitepaper.Shtml](http://www.Cdt.Org/Crypto/CESA/Cesawhitepaper.Shtml)>.

*Court Declares Crypto Restrictions Unconstitutional: Free Speech Trumps Clinton Wiretap Plan*, (last modified Dec. 19, 1996) <[www.eff.org](http://www.eff.org)>.

Courtney Macavinta, *Terrorism Plays Into Net Debate* (visited Mar. 13, 2000) <<http://news.cnet.com/news/>>.

*Cryptography Export Litigation* (visited May 10, 2000) <<http://www.cdt.org/crypto>>.

David Hudson, *Federal Appeals Panel Rules Encryption Source Code is Protected Speech* (last modified Apr. 5, 2000) <<http://www.freedomforum.org/news/2000/04/2000-04-05-05.asp>>.

David Hudson, *Journal Of A Strained Net* (last modified Aug 9, 1996) <<http://www.internetvalley.com/intval.html>>.

*Defense Advanced Research Projects Agency* (visited Feb. 25, 2000)  
<<http://www.darpa.mil/>>.

*Electronic Surveillance -- Title III Affidavits* (visited Nov. 7, 2000)  
<[http://www.usdoj.gov/usao/eousa/foia\\_reading\\_room/usam/title9/crm00029.htm](http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00029.htm)>.

*Electronic Surveillance and the Fourth Amendment* (visited Dec. 29, 2000)  
<<http://caselaw.lp.findlaw.com/data/constitution/amendment04/f132>>.

*Encryption* (visited Mar. 12, 2000)  
<<http://webopedia.internet.com/Networks/Security/Encryption/encryption.html>>.

*General Information About the Electronic Frontier Foundation* (visited Feb. 20, 2000) <<http://www.eff.org/abouteff.html>>.

Gregory R. Gromov, *History of Internet and WWW: The Roads and Crossroads of Internet History* (visited Feb. 24, 2000) <<http://www.internetvalley.com/intval.html>>.

Justin Matlick, *U.S. Encryption Policy: A Free-Market Primer* (visited Mar. 13, 2000) <<http://www.pacificresearch.org>>.

*Mission Statement* (visited Feb. 20, 2000) <<http://www.pacificresearch.org/>>.

Adam Clayton Powell III, *New White House Cryptography Policy Criticized By Industry*, (last modified Nov. 24, 1999)  
<<http://www.freedomforum.org/technology/1999/11/24crypto.asp>>.

*Protecting Military Computer Networks From Internet Threats* (visited Mar. 13, 2000) <<http://www.telos.com/corpinfo/feature/infosec/abstract.html>>.

*Public key cryptography* (visited Mar. 12, 2000)  
<[http://webopedia.internet.com/Networks/Security/Encryption/public\\_key\\_cryptography.html](http://webopedia.internet.com/Networks/Security/Encryption/public_key_cryptography.html)>.

Solveig Bernstein, *Democracy Betrayed Means New Wiretapping Powers* (visited Apr. 20, 2000) <[www.cato.org/dailys](http://www.cato.org/dailys)>.

*Symmetric key* (visited Mar. 12, 2000)  
<[http://webopedia.internet.com/TERM/s/symmetric\\_key\\_cryptography.html](http://webopedia.internet.com/TERM/s/symmetric_key_cryptography.html)>.

Phillip Taylor, *Free-Speech Advocates Say Revised Encryption Regulations Fall Short* (last modified Jan. 20, 2000) <<http://www.freedomforum.org/speech/2000/1/20encryption.asp>>.

*U.S. Export Control Laws And Regulations* (last modified May 11, 1999)  
<<http://www.hq.nasa.gov/office/codei/nasaecp/Webbrfg/tsld009.htm>>.

Vinton Cerf, et al., *A Brief History of the Internet* (visited Feb. 24, 2000)  
<<http://www.isoc.org/internet/history/brief.html>>.

University of British Columbia Theoretical Physics Homepage (visited Dec.2, 2000)  
<<http://axion.physics.ubc.ca/crypt.html#LEGAL>>.

#### **Other**

AMERICAN CIVIL LIBERTIES UNION, *BIG BROTHER IN THE WIRES: WIRETAPPING IN THE DIGITAL AGE* (1998).

ARNOLD G. REINHOLD, *STRONG CRYPTOGRAPHY: THE GLOBAL TIDE OF CHANGE* (CATO INSTITUTE, 1999).

THE CENTER FOR DEMOCRACY AND TECHNOLOGY, *AN OVERVIEW OF CLINTON ADMINISTRATION ENCRYPTION POLICY INITIATIVES* (2000).

THE CENTER FOR DEMOCRACY AND TECHNOLOGY, *POLICY POST VOL. 6 NO.15, A BRIEFING ON PUBLIC POLICY ISSUES AFFECTING CIVIL LIBERTIES ONLINE* (2000).

*Commerce Announces Streamlined Encryption Export Regulations*, United States Department of Commerce press release, Jan. 12, 2000.

Department of Commerce Press Release, *Administration Implements Updated Encryption Export Policy* (last modified January 12, 2000)<<http://osecnt13.osec.doc.gov/public.nsf/docs/60D6B47456BB389F852568640078B6C0>>.

ELECTRONIC PRIVACY INFORMATION CENTER, *CRYPTOGRAPHY AND LIBERTY 1999: AN INT'L SURVEY OF ENCRYPTION POLICY* (1999).

HENRY B. WOLFE, *THE MYTH OF SUPERIORITY OF AMERICAN ENCRYPTION PRODUCTS* (CATO INSTITUTE, BRIEFING PAPER No. 42, 1998).

NATIONAL SECURITY AGENCY, *THREAT AND VULNERABILITY MODEL FOR KEY RECOVERY* (1998).

Reno Calls for Ban on Encryption Products on the Net, *Newbytes PM*, July 28, 1999, available in LEXIS, News Library, Asapii File.

## LIST OF ACRONYMS

ACLU	American Civil Liberties Union
AFI	Air Force Instruction
AFPD	Air Force Policy Directive
BXA	Bureau of Export Administration
CALEA	Communications Assistance for Law Enforcement Act
CESA	Cyberspace Electronic Security Act of 1999
CCL	Commerce Control List
COMSEC	Communications Security
DES	Digital Encryption Standard
DOD	Department of Defense
DOJ	Department of Justice
EAA	Export Administration Act of 1979
EAR	Export Administration Regulations
ECPA	Electronic Communications Privacy Act of 1986
EES	Electronic Encryption Standard
EFF	Electronic Frontier Foundation
EPIC	Electronic Privacy Information Center
FBI	Federal Bureau of Investigation
INFOSEC	Information Security
ITAR	International Traffic in Arms Regulation
NSA	National Security Agency
PGP	Pretty Good Privacy
PROTECT Act	Promote Reliable On-Line Transactions to Encourage Commerce and Trade Act of 1999
SAFE Act	Security and Freedom through Encryption Act
SIGNIT	Signals Intelligence